



举一反三

电脑安全防护技巧总动员



企鹅工作室　吴海燕　张　建◎编著



实战技巧 100多个热点快报+300多个知识小栏目+300多个应用技巧+2000多张步骤图片



光盘特色 配套多媒体超值教学光盘，生动、直观、交互性强，实现与书中知识相互结合、相互补充



图解教学 以图解为主、文字为辅，版式精美、技巧实用，安排6组知识小栏目，信息量大



完美打造 全面讲解电脑加密、黑客防御秘笈、查杀电脑病毒、备份与恢复系统数据、数据拯救与修复等电脑安全防护知识

清华大学出版社

举一反三

电脑安全防护技巧总动员

企鹅工作室　吴海燕　张　建　编　著

清华大学出版社
北　京

内 容 简 介

本书主要针对初、中级读者的需求，从零开始、系统全面地讲解电脑安全防护方面的操作步骤与应用技巧。

全书共分为 14 个专题、两个附录，主要内容包括：电脑使用不留痕迹、将隐藏进行到底、电脑加密无极限、找回丢失的密码、电脑系统安全防护、电脑上网安全防护、做好黑客安全防护、远程控制与黑客扫描、彻底查杀病毒、防火墙完全攻略、木马病毒攻防战、备份与恢复系统数据、备份与恢复私人数据、数据拯救与修复、黑客常用命令、常见木马端口列表。

本书及配套多媒体光盘非常适合初、中级读者选用，也可以作为高职高专相关专业和电脑短训班的培训教材。

图书在版编目(CIP)数据

电脑安全防护技巧总动员/企鹅工作室，吴海燕，张建编著. —北京：清华大学出版社，2009.1

(举一反三)

ISBN 978-7-302-18768-4

Ⅰ. 电…　Ⅱ. ①企…　②吴…　③张…　Ⅲ. 电子计算机—安全技术　Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2008)第 161832 号

责任编辑：邹　杰　张丽娜
封面设计：杨玉兰
责任校对：周剑云
责任印制：

出版发行：清华大学出版社　　**地　址：**北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　编：**100084
社 总 机：010-62770175　　**邮　购：**010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：210×285　**印　张：**17.25　**插　页：**1　**字　数：**639 千字
附光盘 1 张
版　　次：2009 年 1 月第 1 版　　**印　次：**2009 年 1 月第 1 次印刷
印　　数：1~6000
定　　价：38.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　　产品编号：

丛书序

学电脑有很多方法，更有很多技巧。一本好书，不仅能让读者快速掌握基本知识、操作方法，还应让读者能够无师自通、举一反三。

基于上述目的，清华大学出版社精心打造了品牌丛书——“举一反三”。本系列丛书作者精心挑选了最实用、最精炼的内容，采用一个招式对应一个技巧，同时补充讲解一个知识点的叙述方式。此外书中还穿插“内容导航、热点快报、知识补充、注意事项、专家坐堂、举一反三”等众多小栏目，采用双栏、三栏相结合的紧凑排版方式，配合步骤、技巧，以重点、难点相对突出的精美双色印刷，并配套大容量多媒体教学光盘，使读者能够参照书中的实际操作步骤、对照光盘快速开展实战演练，从而达到“举一反三”的目的。

丛书主要内容

如果您是一名电脑初、中级读者，那么“举一反三”丛书正是您所需要的。丛书覆盖面广泛、知识点全面，第一批书目如下所示。

- 《网上冲浪技巧总动员》
- 《Windows Vista 技巧总动员》
- 《Office 2007 办公技巧总动员》
- 《Word 2007 排版及应用技巧总动员》
- 《Excel 2007 表格处理及应用技巧总动员》
- 《系统安装与重装技巧总动员》
- 《数码照片拍摄与处理技巧总动员》
- 《家庭 DV 拍摄与处理技巧总动员》
- 《电脑故障排除技巧总动员》
- 《电脑硬件与软件技巧总动员》
- 《BIOS 与注册表技巧总动员》
- 《电脑安全防护技巧总动员》

丛书主要特色

作为一套面向初、中级读者的系列丛书，“举一反三”丛书具有“内容精炼、技巧实用”，“全程图解、轻松阅读”，“情景教学、快速上手”，“精美排版、双色印刷”，“书盘结合、互补学习”五大特色。

☒ 内容精炼　技巧实用

每本图书均挑选精炼、实用的内容，循序渐进地展开讲解，符合读者由浅入深、逐步提高的学习习惯。语言讲解准确、简明，读者不需要经过复杂的理解和思考，即可明白所学习的知识。

从书以应用技巧为主，操作步骤为辅，理论知识为补充；采用一个招式对应一个技巧，同时补充讲解一个知识点的叙述方式。对于各种需要操作练习的知识，都以操作步骤的方式进行讲解，让读者在大量的操作步骤和应用技巧中，逐步培养动手实践的能力。

☒ 全程图解　轻松阅读

从书采用“全程图解”的讲解方式，在以简洁、清晰的文字对知识内容进行说明后，以图形的表现方式，将各种操作步骤直观地表现出来。基本上是一个操作步骤对应一个图形，且在图形上添加步骤序号与说明，更准确地对各知识点进行操作演示，这样，既节省了版面，又增加了可视性，使读者轻松易学。

☒ 情景教学　快速上手

从书非常注重读者的学习规律和学习心态，安排了“内容导航、热点快报”学习大框架，以及“知识补充、注意事项、专家坐堂、举一反三”等学习小栏目，通过打造一种合理的情景学习方法和模式，在活泼版面、轻松阅读的同时，让读者能够主动思考、触类旁通，从而达到快速上手、举一反三的目的。

☒ 精美排版　双色印刷

从书采用类似杂志的版式设计，使用 10 磅字号、双栏和三栏相结合的排版方式，版式精美、新颖、紧凑，既适合阅读又节省版面，超值实用。

从书以黑色印刷为主，而“操作步骤、操作技巧、重点、难点、知识补充、注意事项、专家坐堂、举一反三”等特殊段落，需要读者加强学习的地方则采用双色印刷，以达到重点突出、直观醒目、轻松阅读的目的。

☒ 书盘结合　互补学习

从书配套多媒体教学光盘，光盘内容与书中知识相互结合并互相补充，而不是简单的重复，具有直观、生动、互动等优点。

丛书特色栏目

笔者在编写本书时，非常注重读者的学习规律和学习心态，每个专题安排了“内容导航、热点快报”等学习大框架，以及“知识补充、注意事项、专家坐堂、举一反三”等学习小栏目，让读者可以更加高效地学习、更加轻松地掌握。

主要栏目	主要内容
内容导航	在每个专题的首页，简明扼要地介绍了本专题将要学习的主要内容，使读者在学习的过程中能够有的放矢
热点快报	对本专题所讲的知识进行更准确、更全面的概括，以精炼的、概括的语言列出本专题将要介绍的重要内容和经典技巧等
知识补充	在众多操作步骤中，穿插一些必备知识，或是本专题主要知识点、重点和难点的学习提示
注意事项	强调本专题的重点、难点，以及学习过程中需要特别注意的一些问题或事项，从而达到巩固知识，融会贯通的目的
专家坐堂	将高手在学习电脑应用过程中积累的经验、心得、教训等通通告诉你，让你快速上手、少走弯路
举一反三	对新概念、新知识、重点、难点和应用技巧通过典型操作加以体现，从而达到触类旁通、举一反三的目的

光盘主要特色

本书配套交互式、多功能、大容量的多媒体教学光盘。书中涉及的主要内容，通过演示光盘作了必要的示范。光盘内容与图书内容相互结合并互相补充，既可以对照光盘轻松自学，又可以参照图书互动学习。配套光盘具有以下特色。

光盘特色	主要内容
功能强大	配套光盘具有视频播放、人物情景对话、背景音乐更换、音量调节、光盘目录快速切换等众多功能模块，功能强大、界面美观、使用方便
情景教学	配套光盘通过老师、学生和小精灵 3 个卡通人物来再现真实的学习过程，情景教学、生动有趣
互动学习	读者可跟随光盘的提示，在光盘演示中执行如单击、双击、输入、拖动等操作，实现现场互动学习的新模式
边学边练	将光盘切换成一个文字演示窗口，读者可以根据文字说明和语音讲解的指导，在电脑中进行同步跟练操作，边学边练

丛书创作团队

丛书由“企鹅工作室”集体创作，参与编写的人员有张建、张璇、王涛、李天珍、包婵娟、朱春英、朱志明、吴琪菊、吴海燕、余素芬、周玲、张顺德、赵敏捷、费一峰、毛向城、陈飞、彭文芳等。

由于时间仓促和水平有限，书中难免有疏漏和不妥之处，敬请广大读者批评指正，读者服务邮箱：ruby1204@gmail.com。

企鹅工作室

前言



学电脑有很多方法，更有很多技巧。

本书主要针对初、中级读者的需求，从零开始、系统全面地讲解了电脑安全防护方面的操作步骤与应用技巧。

本书主要内容

全书精心安排了 14 个专题、两个附录的内容，以应用技巧为主，操作步骤为辅，一个技巧对应一个知识点，具体内容如下表所示。

本书专题	主要内容
专题一　电脑使用不留痕迹	介绍 WinRAR 访问记录、IE 访问记录、QQ 与 MSN 使用记录、Media Player 播放记录以及托盘区图标记录的清除等技巧
专题二　将隐藏进行到底	介绍隐藏文件、隐藏图标、隐藏 QQ、伪装私人文件夹、伪装记事本、伪装 IP 等技巧
专题三　电脑加密无极限	介绍开机、登录、电源、Word 文档、Excel 文档、Access 文档和 WinRAR 压缩软件等相关密码的设置技巧
专题四　找回丢失的密码	介绍破解 CMOS 密码、找回 WinZIP 与 WinRAR 密码、找回 DF 与 QQ 密码、制作密码重置盘等技巧
专题五　电脑系统安全防护	介绍伪装陷阱账户、禁止更改文件位置、打造安全 U 盘、锁定桌面，以及做好磁盘检查与系统优化等技巧
专题六　电脑上网安全防护	介绍设置 Cookie 的访问权限、禁用选项卡、恢复 IE、详述了超级兔子的应用和 360 保险箱的应用等技巧
专题七　做好黑客安全防护	介绍查看 IP 地址、绑定列表、检查文件拓展名、防范 IPC$入侵、监控磁盘空间等技巧
专题八　玩转远程控制与黑客扫描	介绍 QQ 远程控制、Super Silent Manager 远程监视、Magic Packet 远程唤醒等技巧
专题九　彻底查杀病毒	介绍金山毒霸查杀病毒与木马、360 安全卫士查杀、瑞星杀毒软件应用等技巧
专题十　防火墙完全攻略	介绍金山网镖 2008 的应用、瑞星个人防火墙 2008 的设置、傲盾 DDOS 防火墙的设置、江民防火墙的设置与升级、龙盾 IIS 和 360ARP 防火墙的设置等技巧



续表

本书专题	主要内容
专题十一 木马病毒攻防战	介绍常见木马分类、顽固木马查杀、电脑病毒感染判断等技巧
专题十二 备份与恢复系统数据	介绍创建系统还原点、备份系统盘、备份还原重要文件、备份与恢复注册表、备份与刷新 BIOS，还介绍使用 Windows 优化大师和驱动精灵备份和恢复驱动程序
专题十三 备份与恢复私人数据	介绍备份与还原 QQ 聊天记录及 QQ 表情、备份与还原 Cookies 以及备份与恢复搜狗输入法等技巧
专题十四 数据拯救与修复	介绍使用 EasyRecovery 恢复数据与文件，以及使用 FinalData 恢复数据与文件等
附录一 黑客常用命令	介绍黑客常用命令
附录二 常见木马端口列表	介绍常见木马端口列表

本书读者定位

本书及配套多媒体光盘非常适合初、中级读者选用，也可以作为高职高专相关专业和电脑短训班的培训教材。

本书还适合以下读者：

- 电脑初中级用户
- 电脑安全防护初级学习者
- 电脑安全防护终极技巧爱好者
- 在校学生与办公人员
- 老年朋友们
- 电脑爱好者与玩家

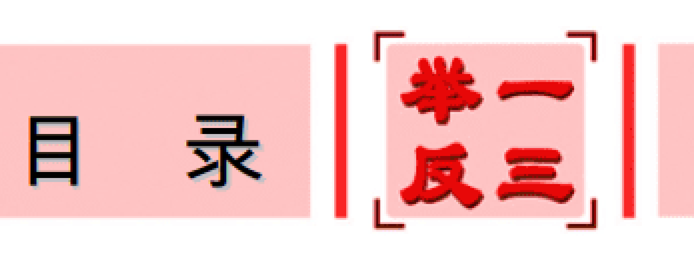
企鹅工作室





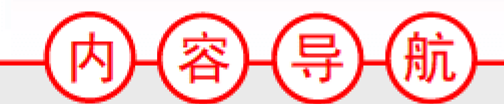



举一
反三


举一
反三



专题一　电脑使用不留痕迹



Windows Vista 系统会把用户操作电脑的过程记录下来，而这些信息很容易泄露个人的隐私。用户的计算机一旦被黑客入侵，其个人隐私将毫无保留地暴露在黑客面前。因此，用户要养成清理使用痕迹的习惯。

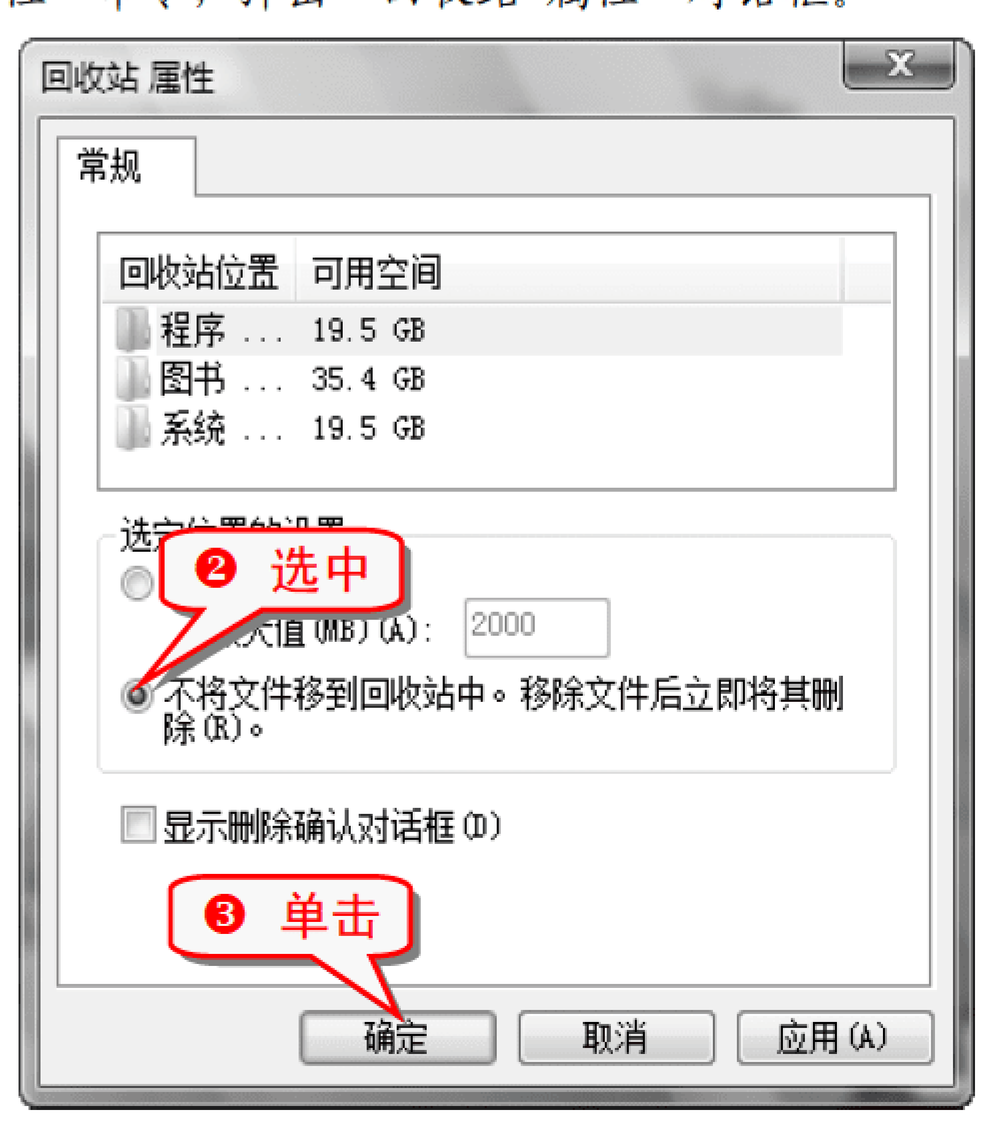
热点快报

- 清除程序使用痕迹
- 清空临时文件夹
- 彻底删除文件技巧
- 清除 IE 上网痕迹
- 清除 QQ 使用记录
- 清除播放器使用记录

技巧1　彻底删除文件

平常删除文件的方式不是真正的删除，时不时地清空回收站又很麻烦，要做到彻底删除文件其实也很简单。

❶ 右击"回收站"图标，在弹出的快捷菜单中选择"属性"命令，弹出"回收站 属性"对话框。



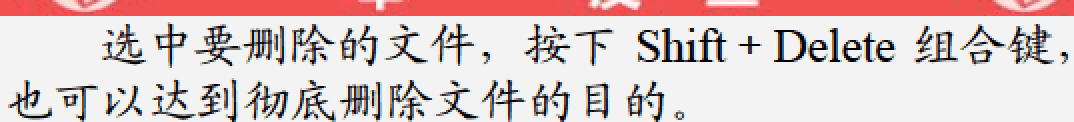
举一反三

选中要删除的文件，按下 Shift＋Delete 组合键，也可以达到彻底删除文件的目的。

专家坐堂

彻底删除文件最保险的方法是从网上下载一个专门的文件删除工具，此类工具有：PowerRMV、XDel Box、360FileKill 以及 Unlocker 等。

技巧2　隐藏"快速启动"工具栏



"快速启动"工具栏中存放的都是常用程序的快捷方式，如果觉得不需要，可以将"快速启动"工具栏隐藏。

❶ 右击任务栏的空白地方，弹出如下图所示的快捷菜单。



举一反三

想要添加"快速启动"工具栏，只需重新选中"快速启动"命令即可。

技巧3 删除「开始」菜单的程序图标

在电脑中安装了应用程序之后，在「开始」菜单的“所有程序”中都可以看到，完全可以将这些程序图标移出「开始」菜单。

❶ 选择“开始”→“所有程序”命令。



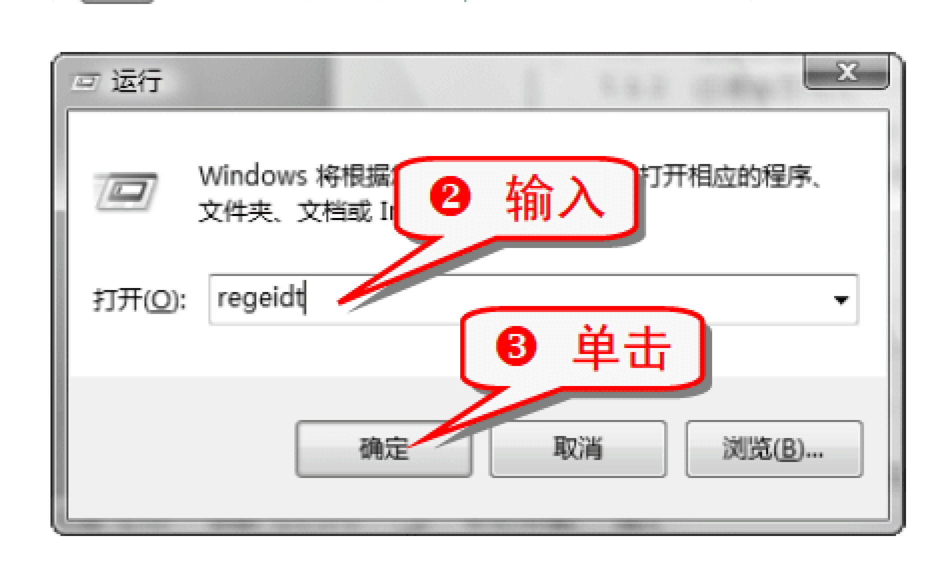
注 意 事 项

从「开始」菜单删除程序图标，对程序本身没有任何影响，相当于删除快捷方式。

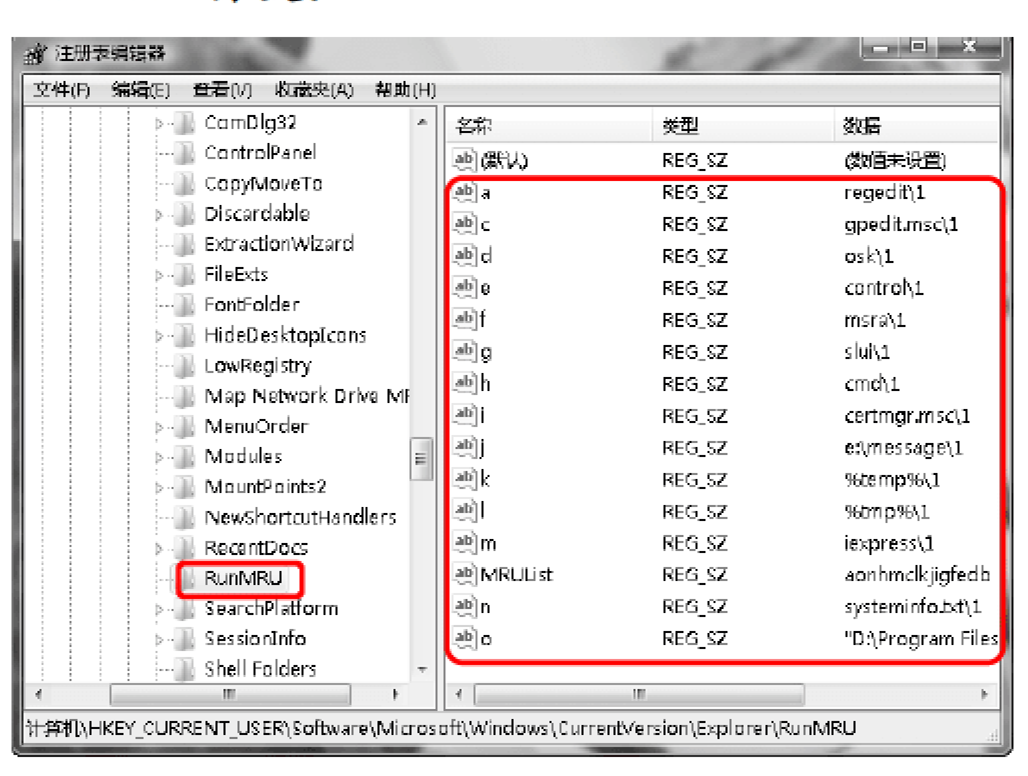
技巧4 选择性清除“运行”历史记录

“运行”对话框的“打开”下拉列表中会记录以前输入的命令，利用注册表编辑器可以有选择地删除这些历史记录。

❶ 按下 [Win] + R 组合键，弹出“运行”对话框。



❹ 在弹出的注册表编辑器中展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU 分支。

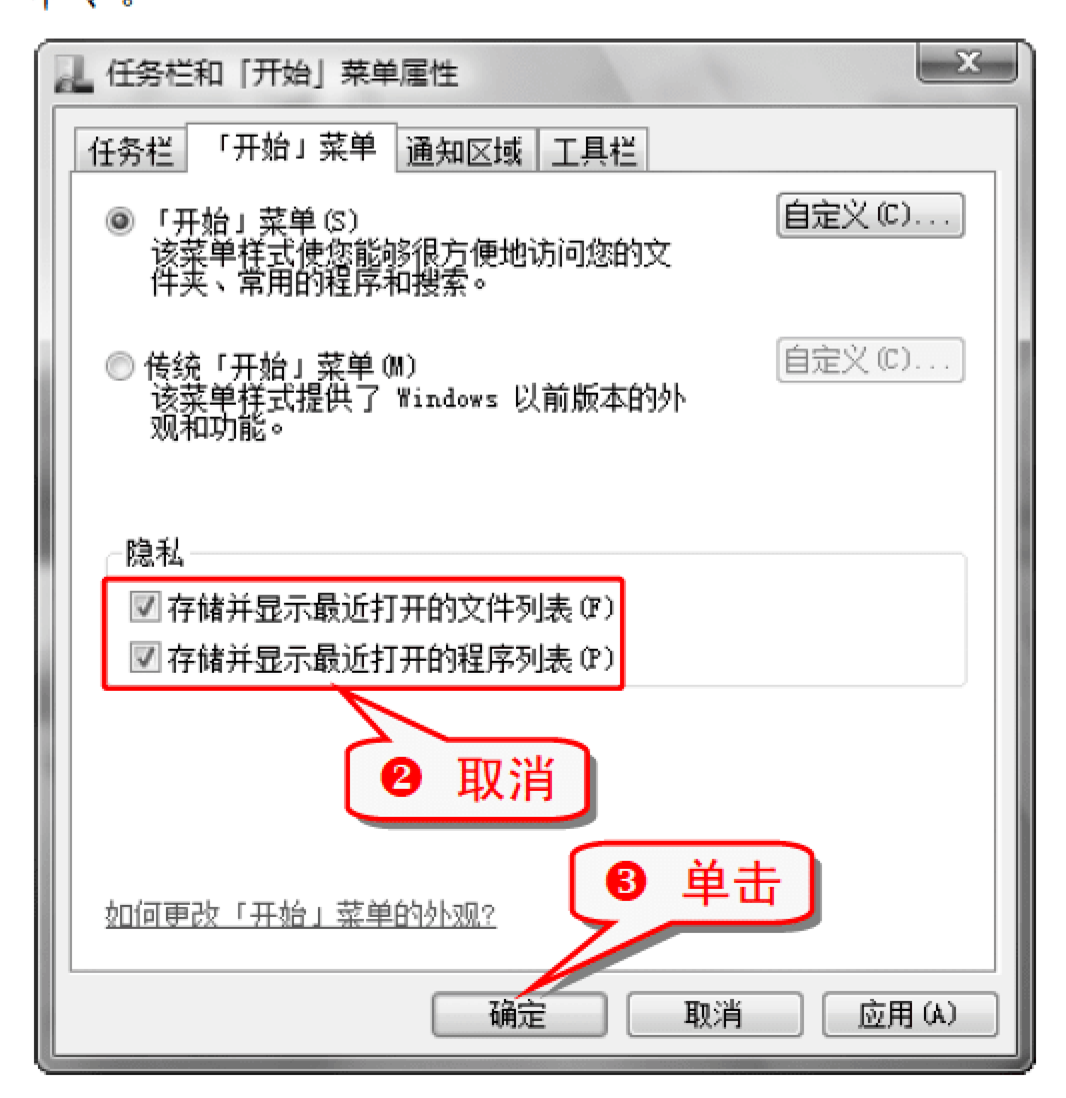


❺ 在右窗格中进行有选择的删除。

技巧5 隐藏程序和文档的使用痕迹

默认情况下，Windows Vista 系统会记录最近访问过的程序和文档的使用痕迹，从而会泄漏隐私，通过简单的设置可以让系统不再记录最近访问的程序和文档的使用痕迹。

❶ 右击“开始”按钮，在弹出的快捷菜单中选择“属性”命令。



注 意 事 项

上述设置不能删除以前的程序和文档的使用痕迹。

技巧6 防止剪贴板泄密

剪贴板是系统临时存放复制信息的地方。当复制粘贴文件时，系统会自动开辟一个空间，把将要复制的内容暂时存放在里面，并且剪贴板中总是保存着最近一次复制的内容，剪贴板是系统不可忽视的安全漏洞。

要清除剪贴板中的内容，可以通过对无用的内容进行复制，以覆盖以前的内容。不过最稳妥的方法是注销当前的用户或者重新启动电脑。

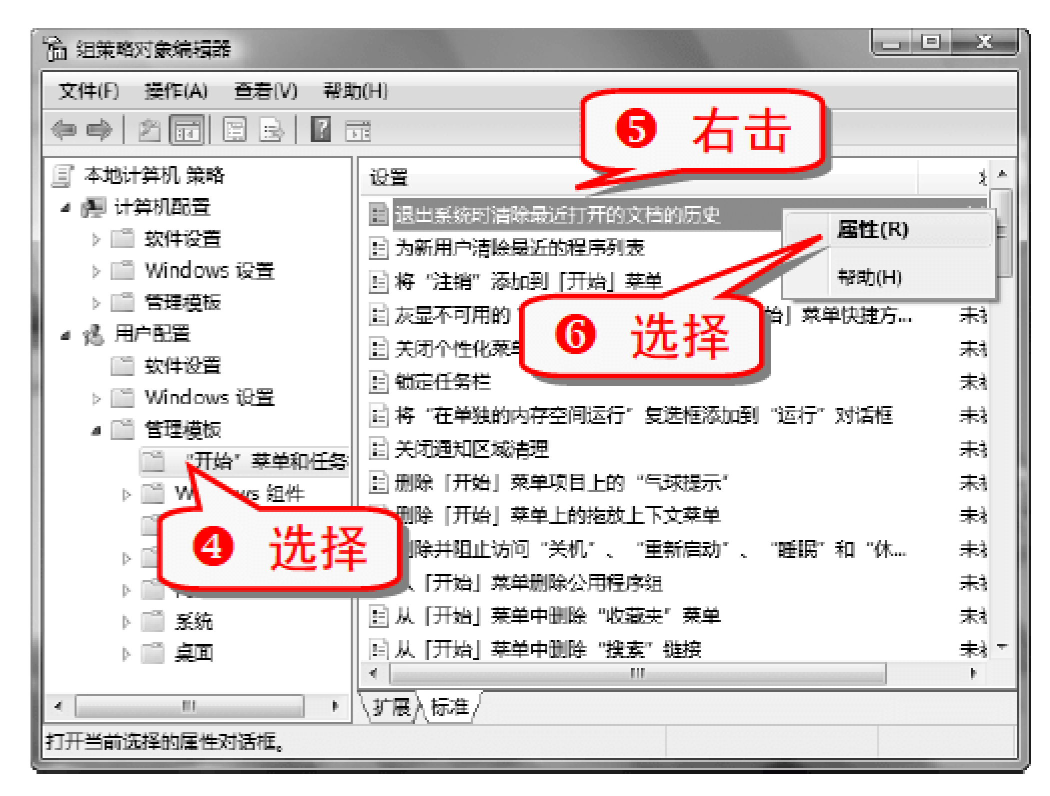
技巧7 清除程序和文档的使用痕迹

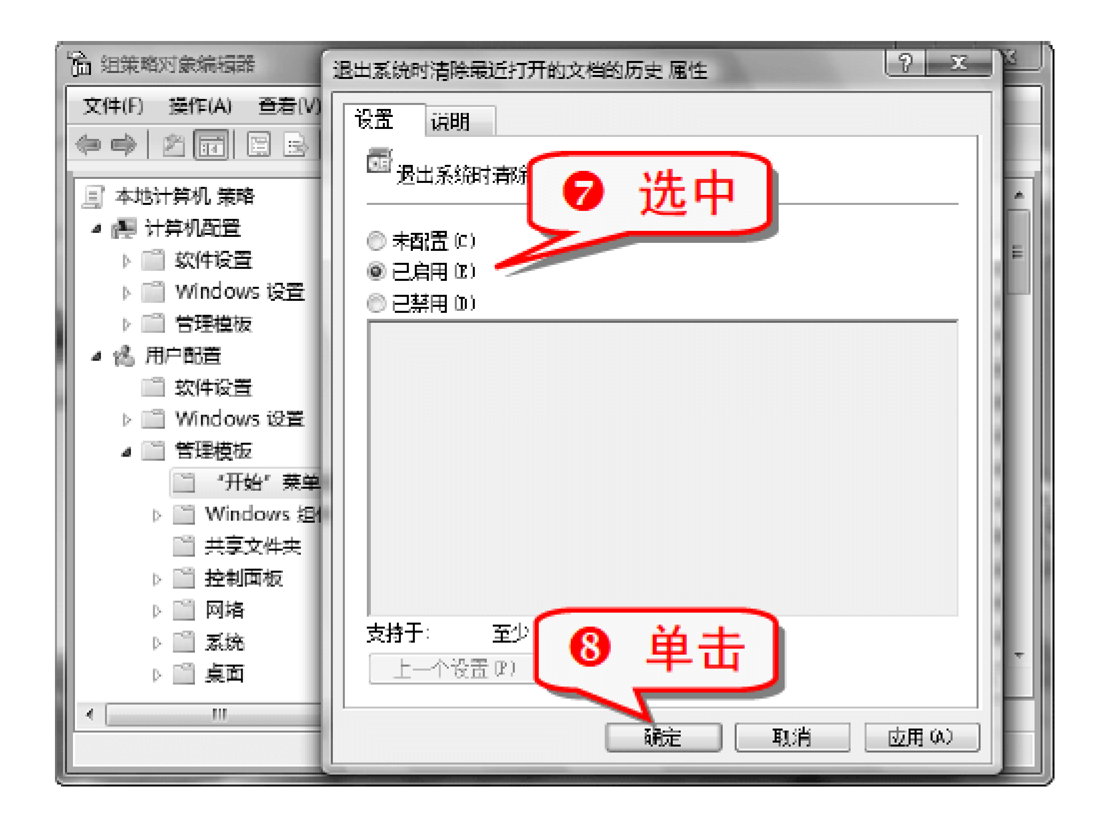
在 Windows Vista 系统中可以通过组策略对象编辑器，彻底清除最近的程序和文档的使用痕迹。

❶ 选择“开始”→“所有程序”→“附件”→“运行”命令，弹出“运行”对话框。









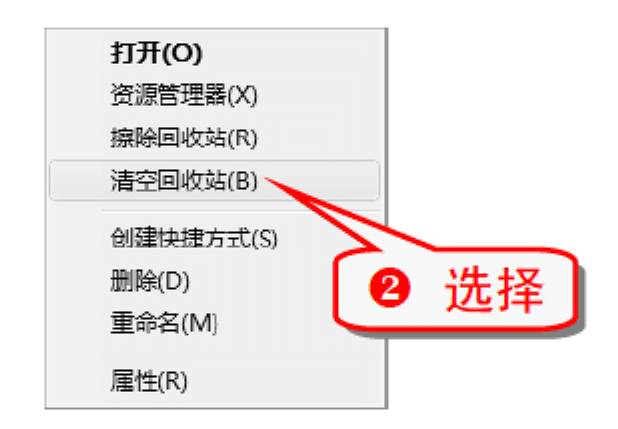
❾ 对“为新用户清除最近的程序列表”也用同样的方式进行设置。

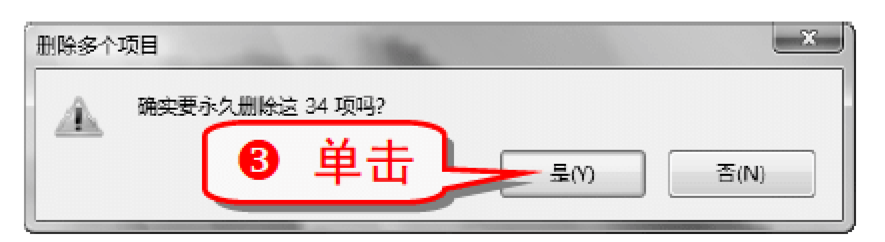
技巧8　及时清空回收站

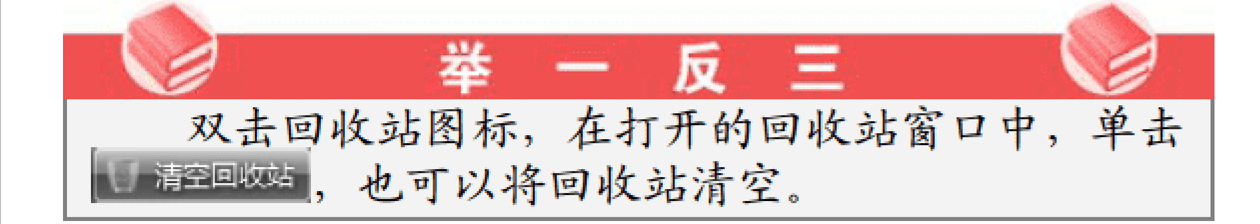
回收站是系统用来存储被删除文件的地方。在实际操作过程中，删除一个文件并不是真正地删除，而是先将其存储在回收站中，以后随时可以从回收站中恢复该文件。

平时要养成清空回收站的习惯，否则会让黑客有可乘之机。

❶ 右击回收站图标，弹出如下图所示的快捷菜单。







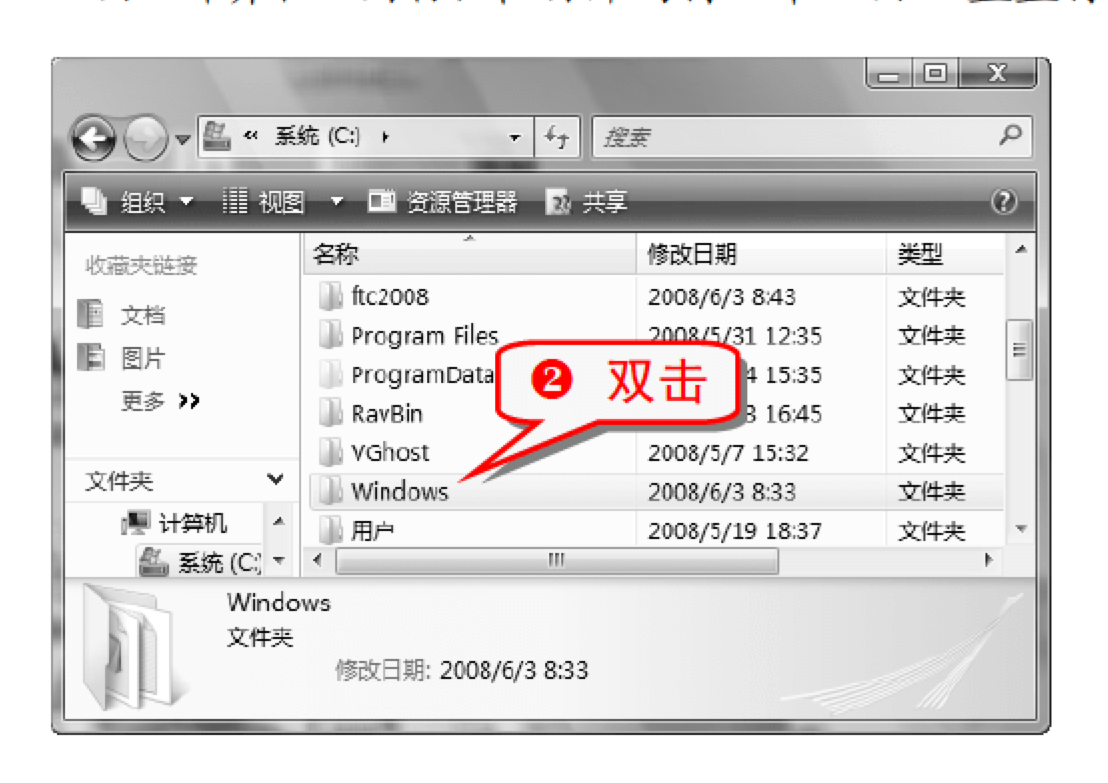
双击回收站图标，在打开的回收站窗口中，单击 清空回收站 ，也可以将回收站清空。

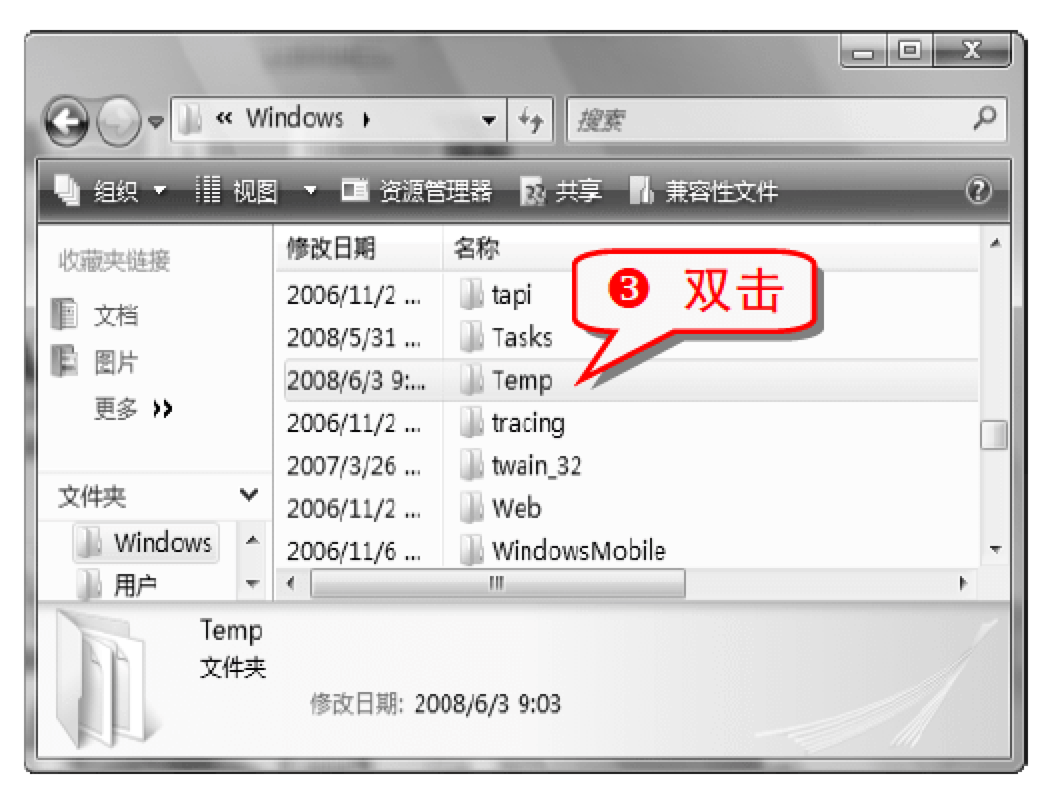
技巧9　手动清空 Windows 临时文件夹

在 Windows 系统运行或安装软件的时候，会生成一些临时文件，这些文件保存在系统的临时文件夹中。此外，有很多文件不会随程序关闭而删除，删除这些临时文件很有必要。

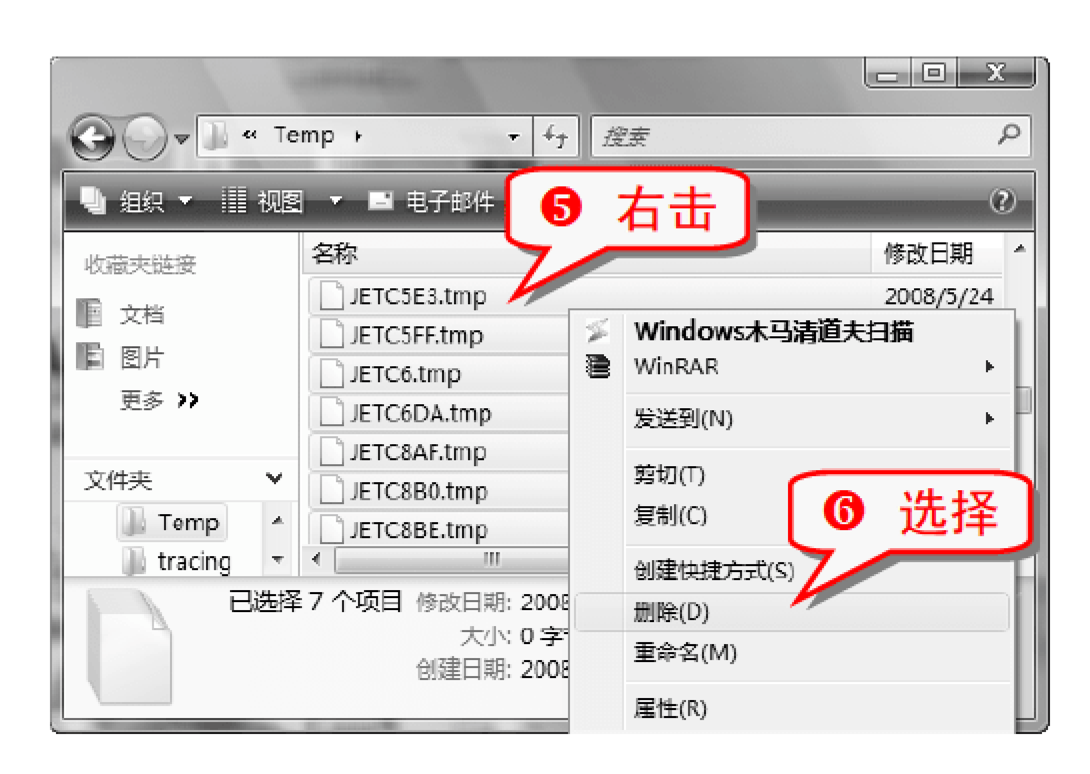
Windows Vista 中的 Temp 文件夹位于 C:\Windows 目录下，打开 Temp 文件夹，删除其中的所有文件即可。

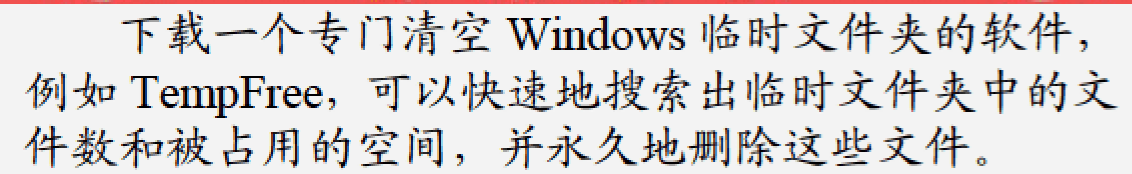
❶ 双击“计算机”图标，在打开的窗口中双击 C 盘盘符。











下载一个专门清空 Windows 临时文件夹的软件，例如 TempFree，可以快速地搜索出临时文件夹中的文件数和被占用的空间，并永久地删除这些文件。

举 一 反 三

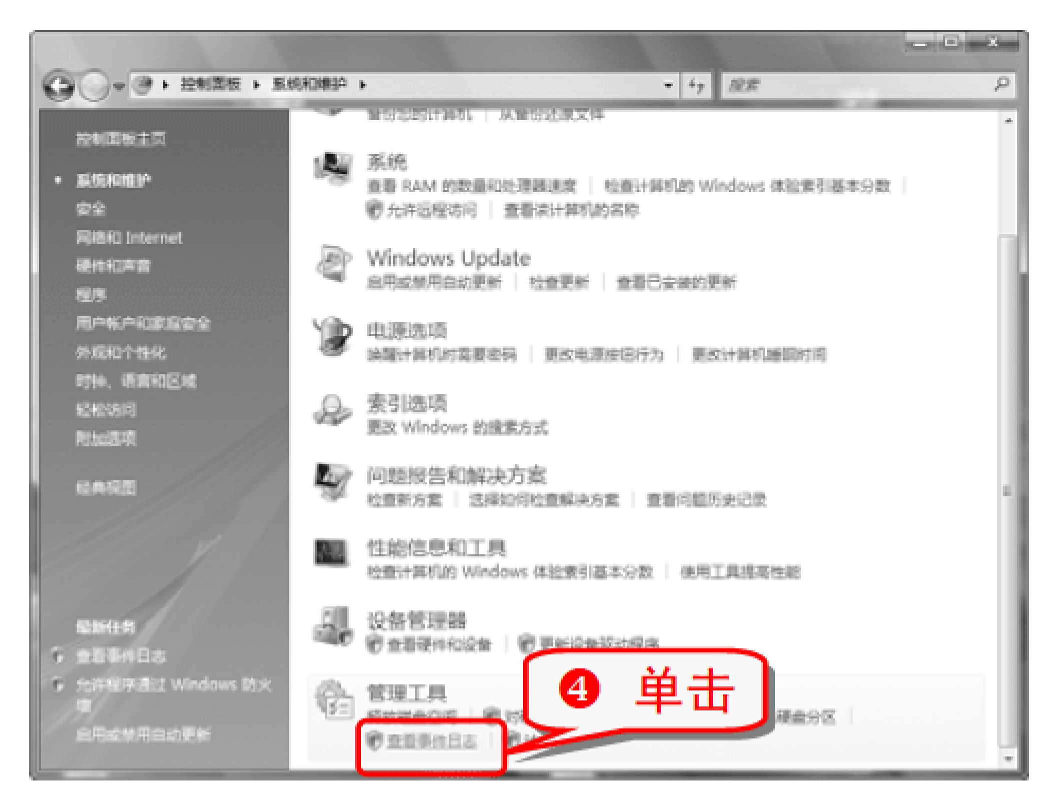
打开“运行”对话框，输入 cmd，打开命令提示符窗口。在命令提示符下，输入 cd /d %temp%后按下 Enter 键，然后再输入 del *.* /s，按下 Enter 键，这样也可以清空 Windows 临时文件夹。

技巧10 清除 Windows 日志文件

日志文件记录着系统发生的一切操作，黑客可以通过系统日志知道用户在什么时间做了什么事情。下面介绍清除 Windows Vista 的日志文件的方法。

❶ 选择“开始”→“控制面板”命令，打开“控制面板”窗口。





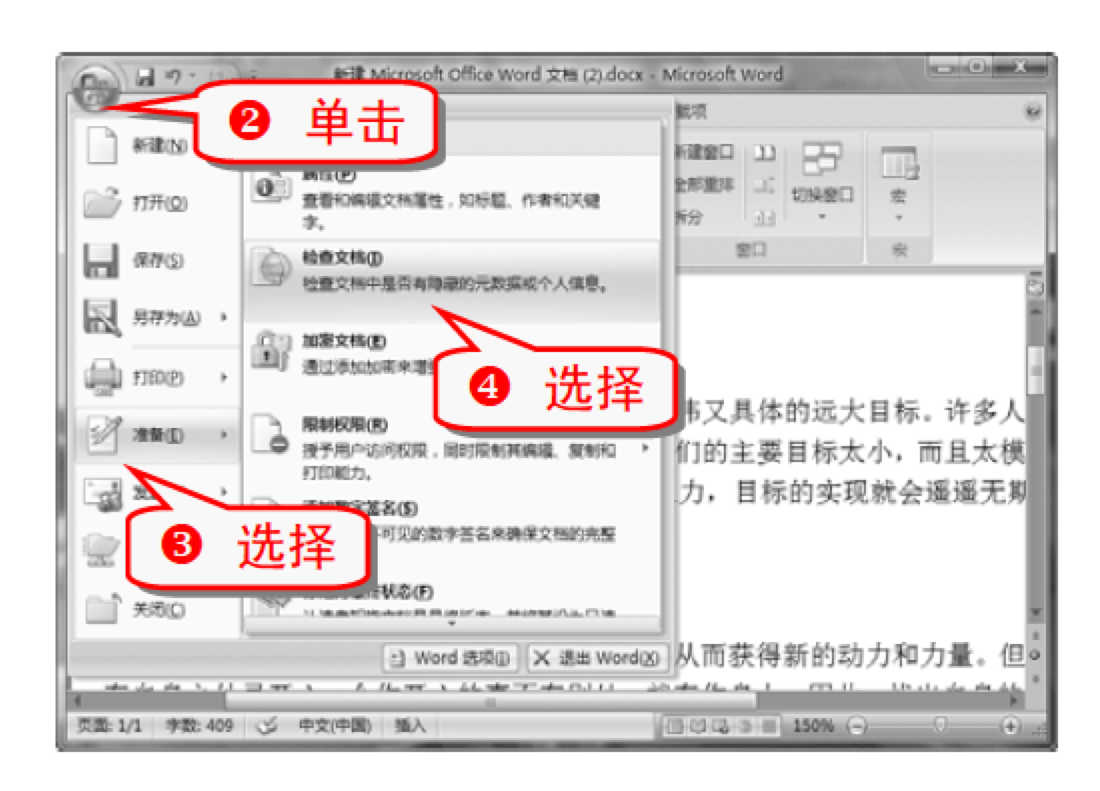


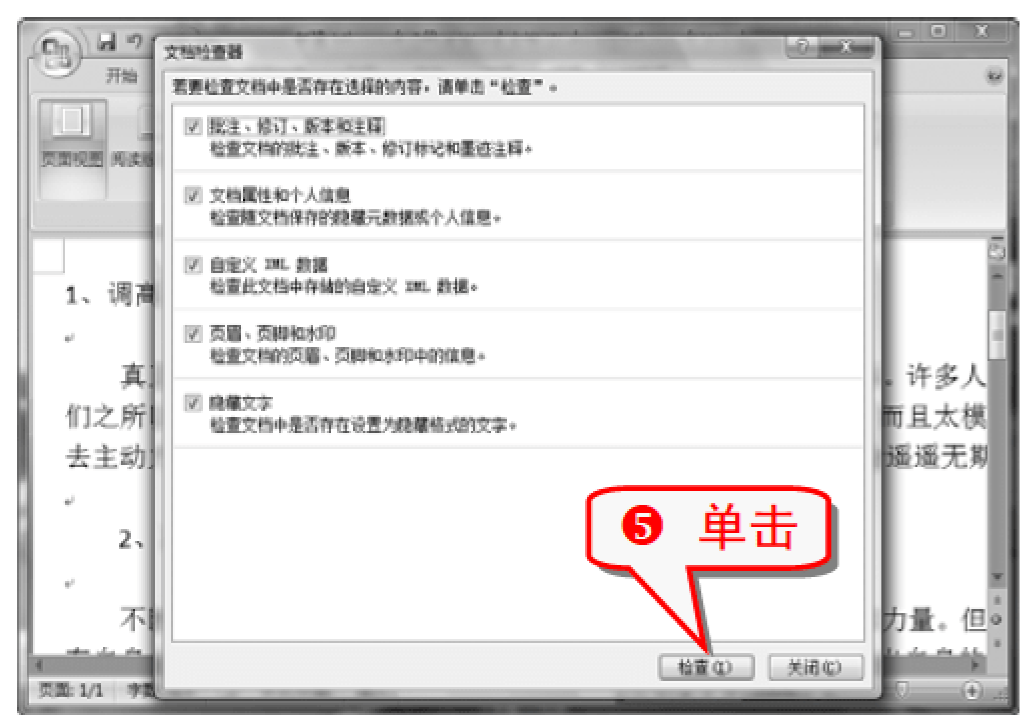
技巧11 清除 Word 文档隐私信息

通过查看 Word 2007 文档属性可以得到文档的标题、主题、作者、创建时间以及最后一次保存的日期等私人信息。Word 2007 中的“检查文档”功能，是 Word 2007 自带的隐私清除工具。

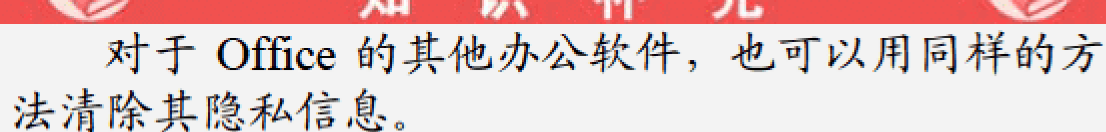
❶ 打开 Word 2007 文档。











对于 Office 的其他办公软件，也可以用同样的方法清除其隐私信息。

技巧12　使 WinRAR 不保留文件历史记录

多次使用压缩软件进行压缩和解压缩操作后，在“文件”菜单中会保留使用过的文件记录。通过下面的步骤可以让 WinRAR 不保留档案文件的历史记录。

❶ 打开 WinRAR 工作界面。

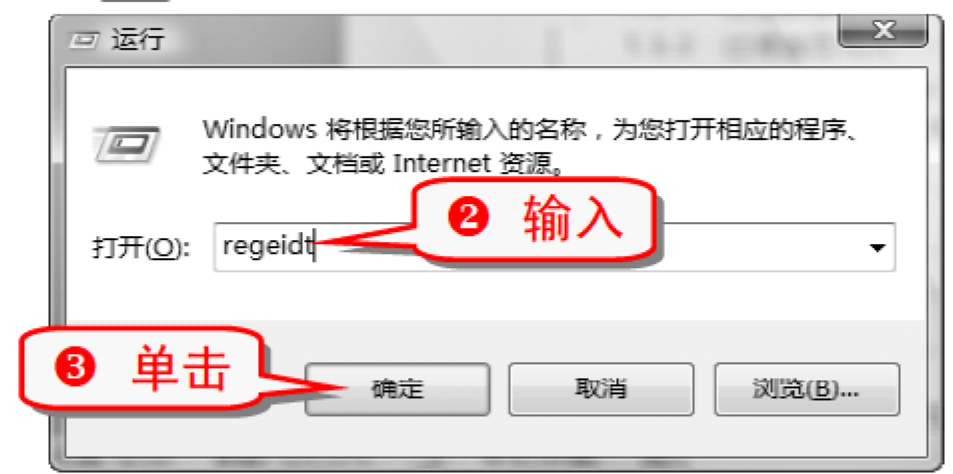




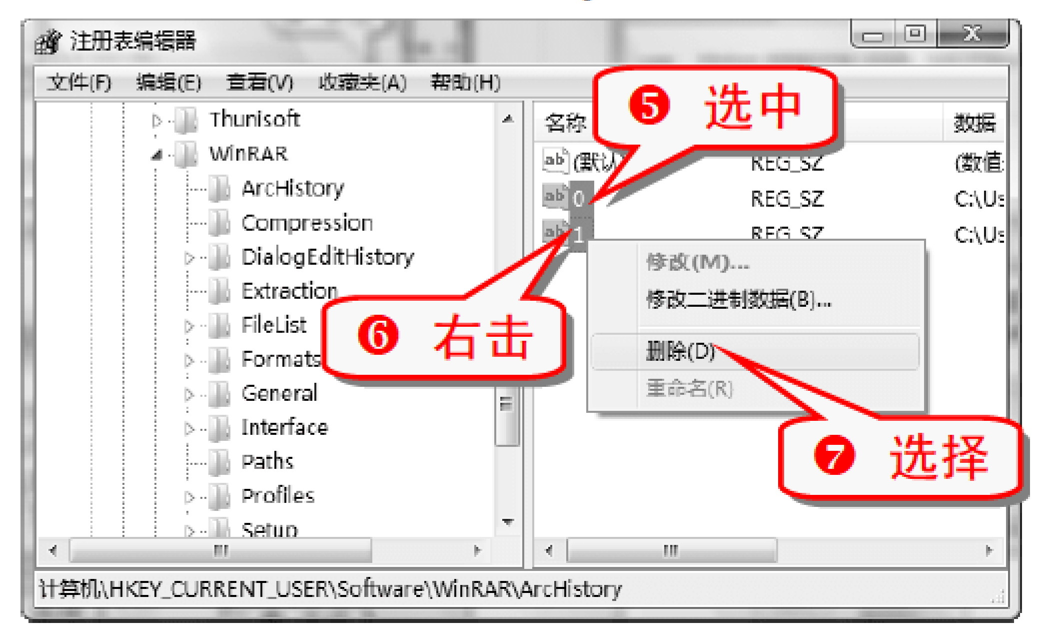
技巧13　清除 WinRAR 访问的历史记录

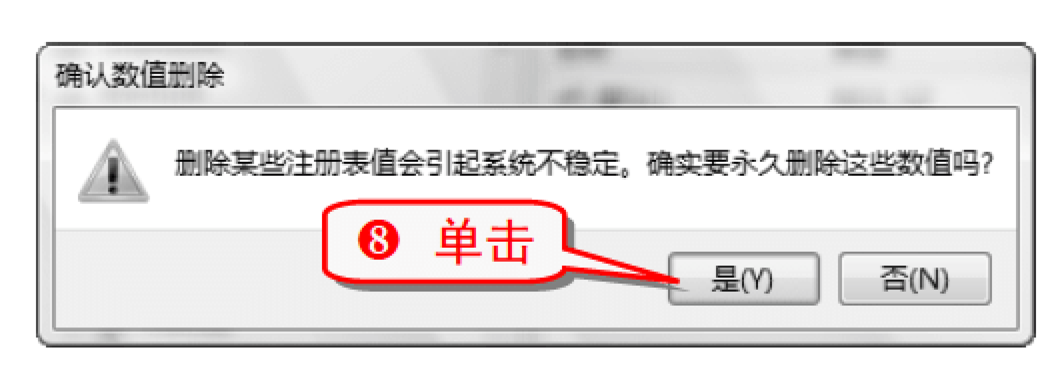
通过对注册表的修改可以将 WinRAR 最近访问的历史记录删除干净。

❶ 按下 [Win] + R 组合键，弹出“运行”对话框。



❹ 在弹出的注册表编辑器中展开 HKEY_CURRENT_USER\Software\WinRAR\ArcHistory 分支。





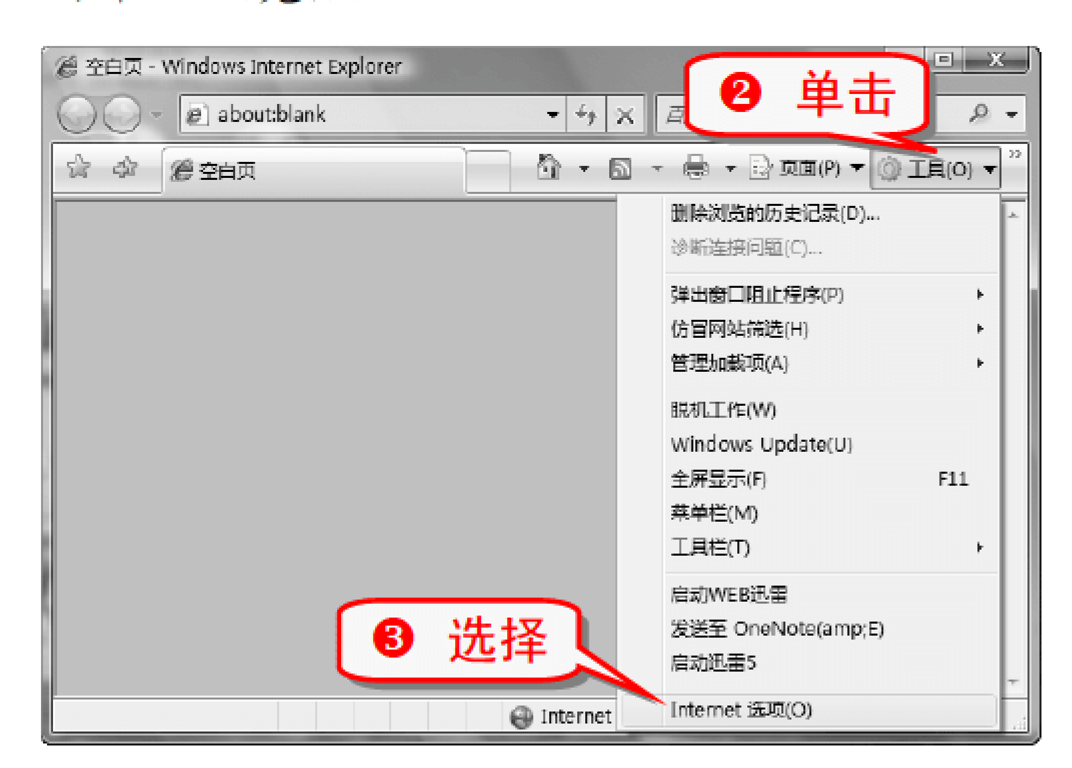
注 意 事 项

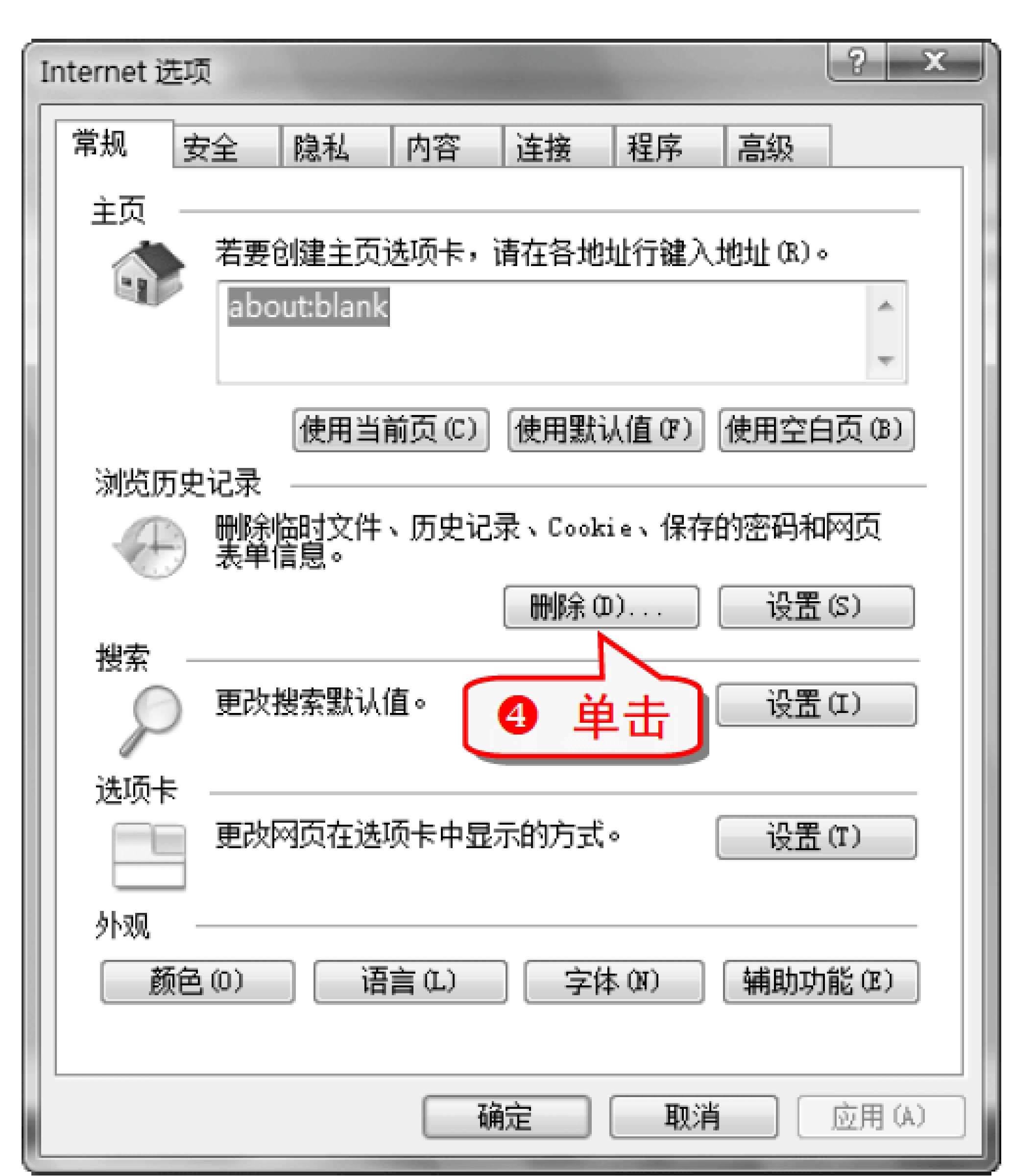
在修改注册表前，请先对注册表进行备份，以免造成不可挽救的后果。

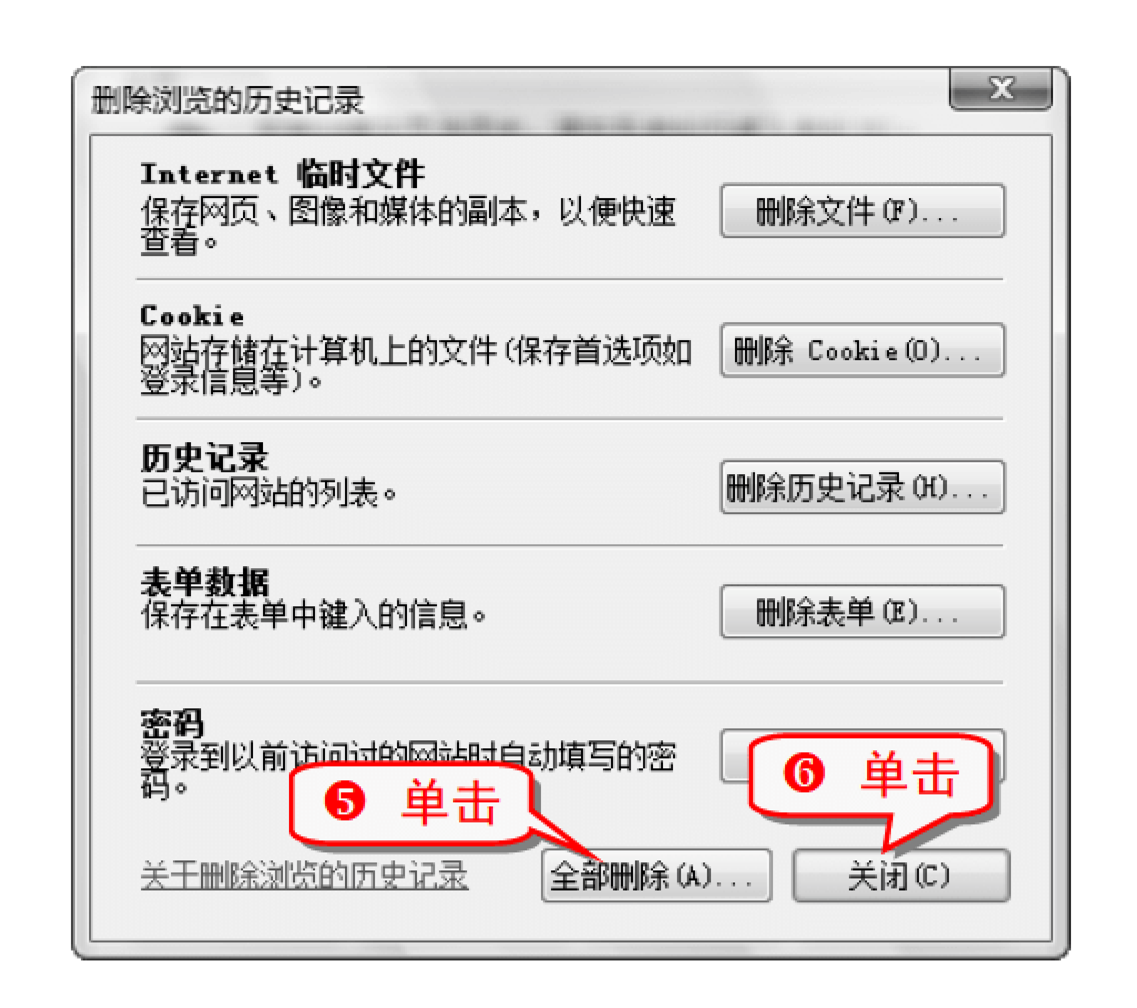
技巧14 清除 IE 上网痕迹

IE 会把最近浏览过网站的临时文件、历史记录、保存的密码和网页表单等信息保存在电脑中，这样很容易泄漏个人隐私，因此要定期将其删除。

❶ 打开 IE 浏览器。







技巧15 手动删除 Cookies 数据

Cookies 是 Web 服务器发送到浏览者电脑中的数据文件，用来提升下次浏览网站的速度。但是 Cookies 的功能可能会被黑客所窃取，并利用其去做一些非法的事情。下面介绍手动删除 Cookies 数据的方法。

❶ 在 Windows Vista 中打开路径为“C:\用户\user”的 Cookies 文件夹。



注 意 事 项

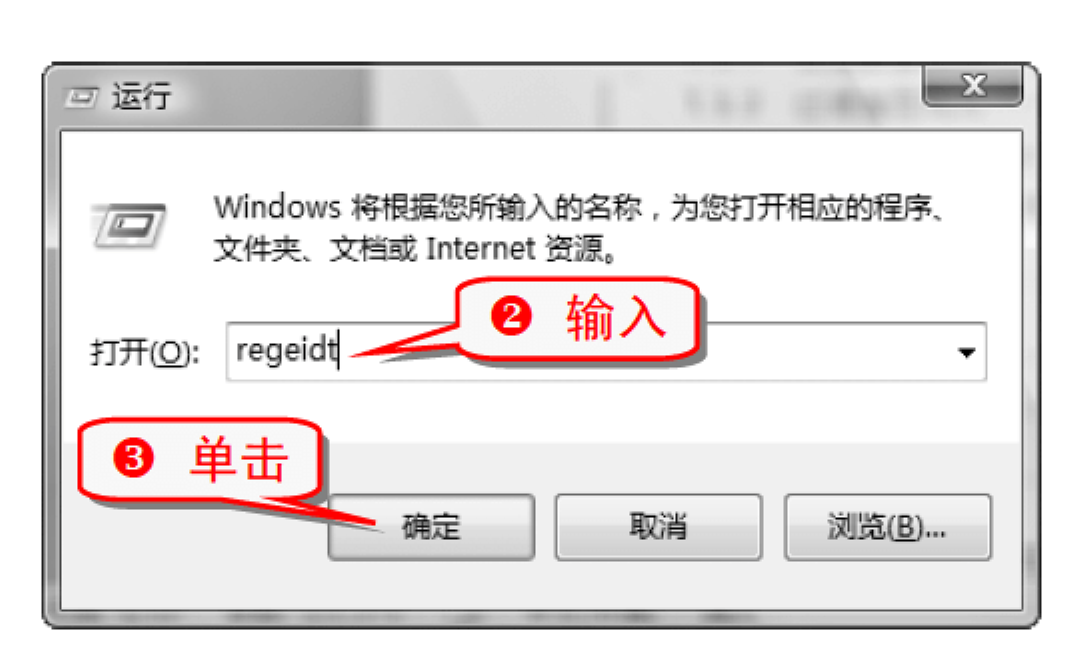
在 Cookies 文件夹下的“Index.dat”文件是系统自身的文件，不能被删除。

技巧16 通过注册表完全禁止 Cookies

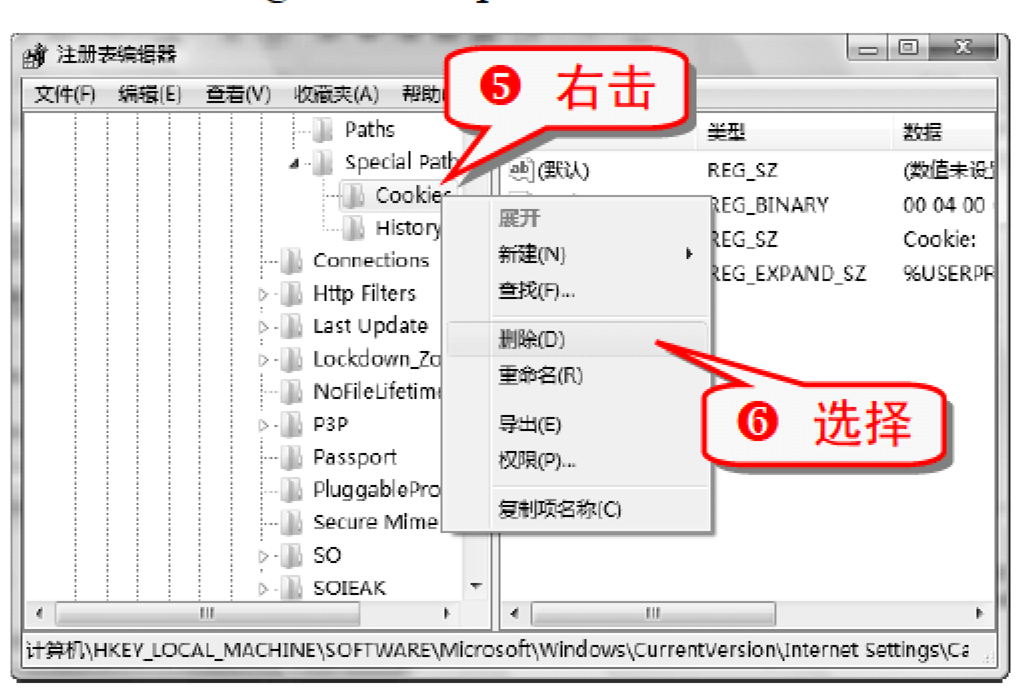
Cookies 删除了之后，只要访问网页，还是会产生 Cookies 文件，如果不想让 Cookies 泄露秘密，那么最彻底的方法就是完全禁止 Cookies。

❶ 按下⊞+R 组合键，弹出“运行”对话框。





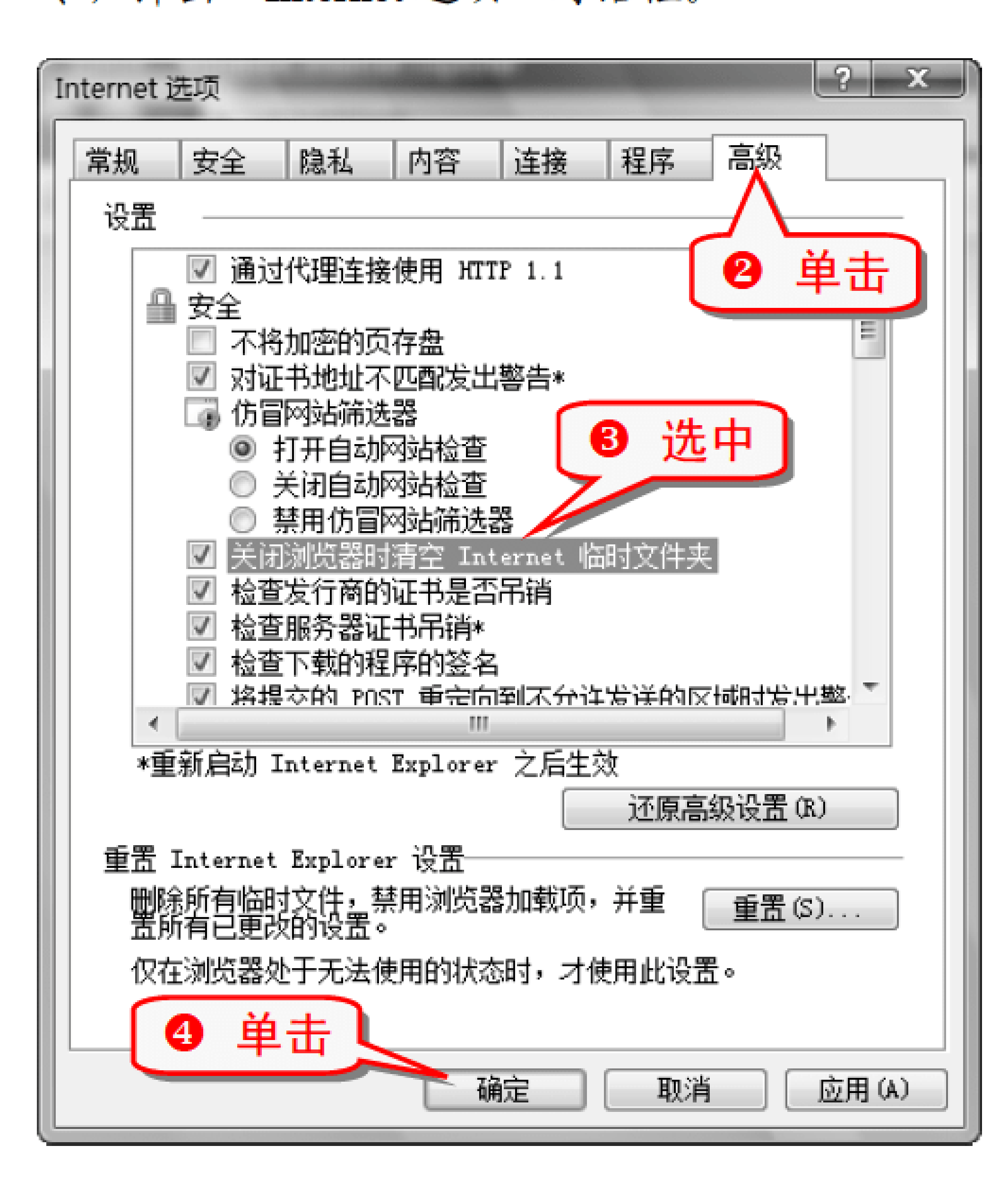
❹ 在弹出的注册表编辑器中展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\Cache\SpecialPaths\Cookies 分支。



技巧17　使 IE 自动清除临时文件夹

手动清除 IE 临时文件夹既费时又费力，设置 IE 自动清除临时文件夹功能将带来极大的方便。

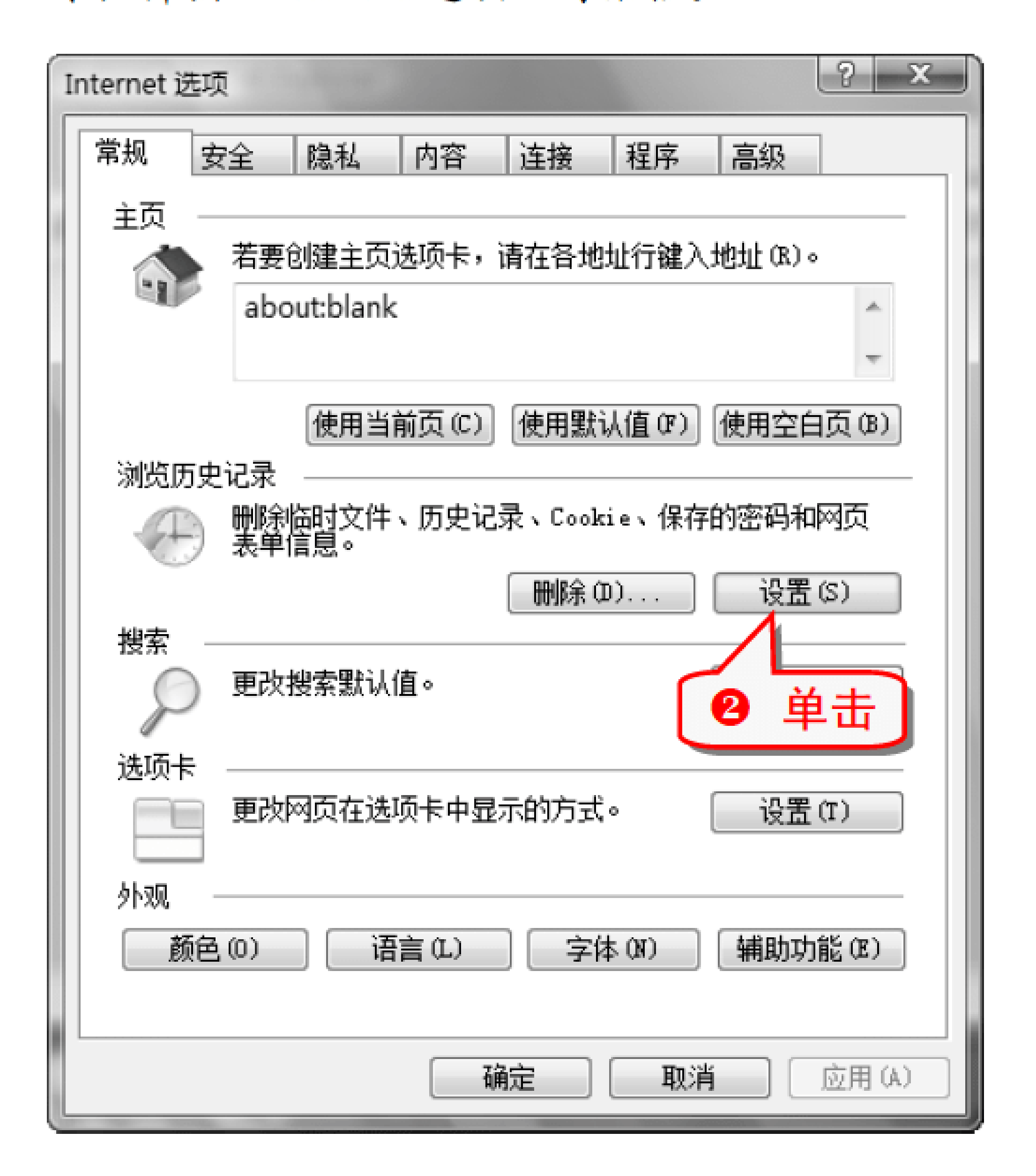
❶ 打开 IE 浏览器，选择"工具"→"Internet 选项"命令，弹出"Internet 选项"对话框。

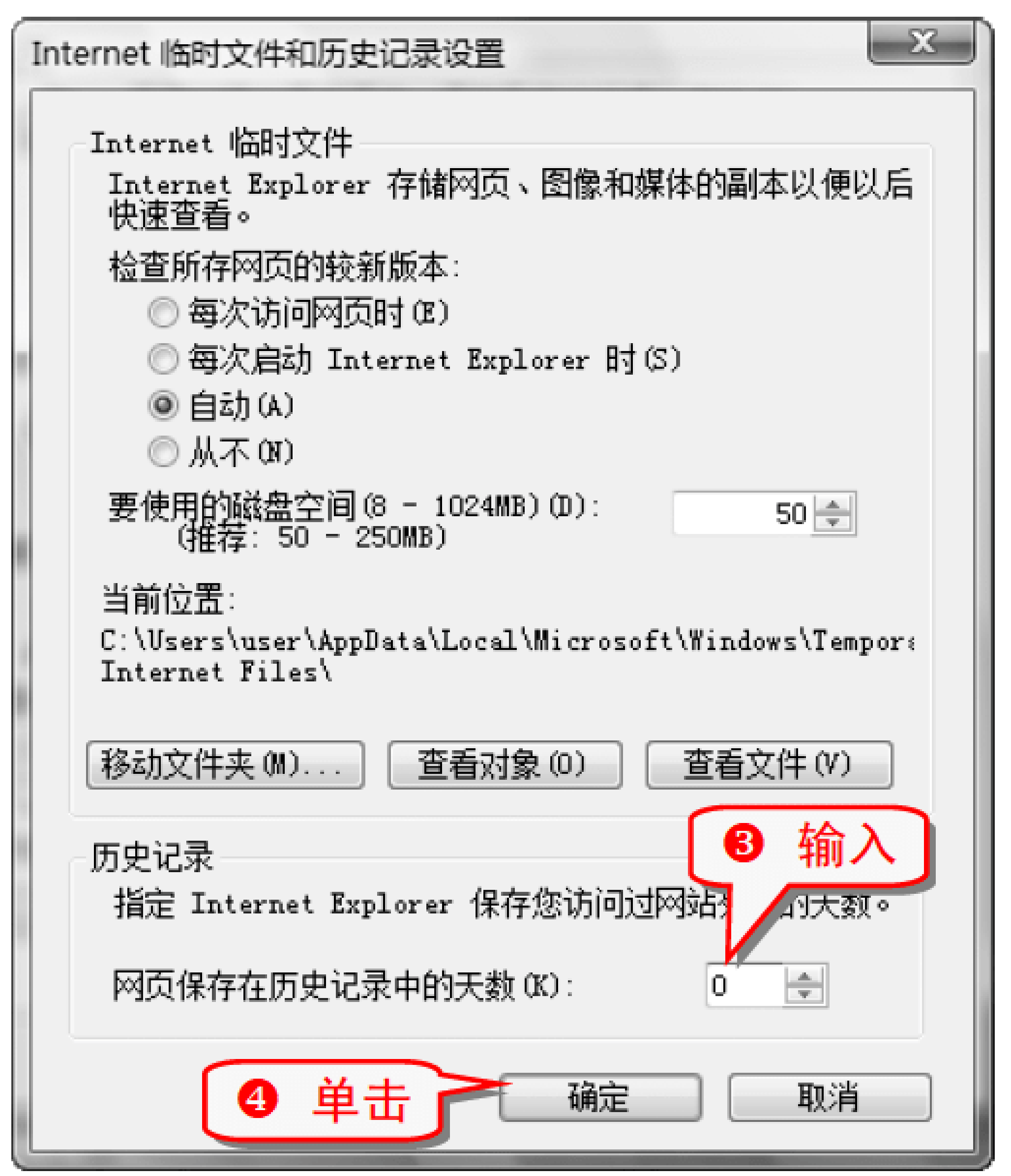


技巧18　使 IE 不再记录访问历史

IE 的历史记录功能确实能为上网带来方便，但是也有不利之处，访问过的历史网页都被记录。虽然可以通过删除历史记录消除上网痕迹，但是最彻底的方法还是让 IE 不再记录访问历史。

❶ 打开 IE 浏览器，选择"工具"→"Internet 选项"命令，弹出"Internet 选项"对话框。

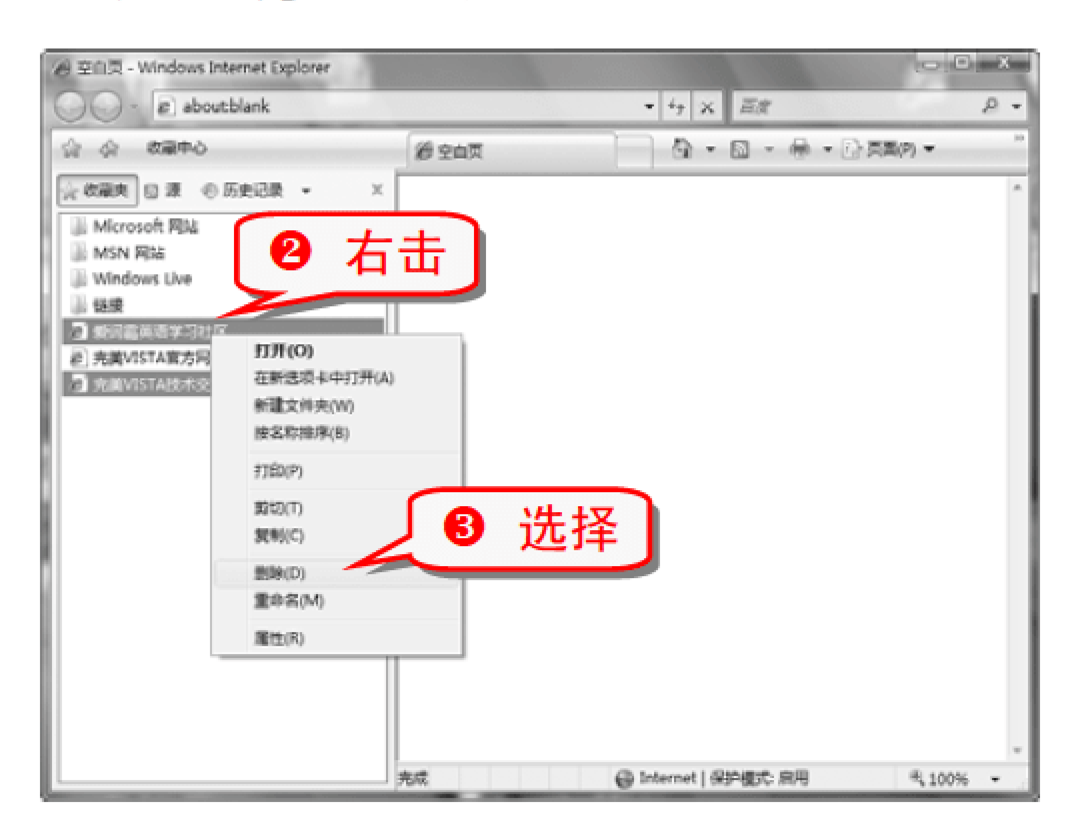




技巧19 清除 IE 收藏夹的收藏记录

IE 收藏夹是收藏与管理网址的地方，上网时遇到精彩的网站，可以将其添加到收藏夹内，以后可以直接从收藏夹中打开这些网站。这些网址记录也会泄露个人隐私，对于不需要的网址记录，有必要将其删除。

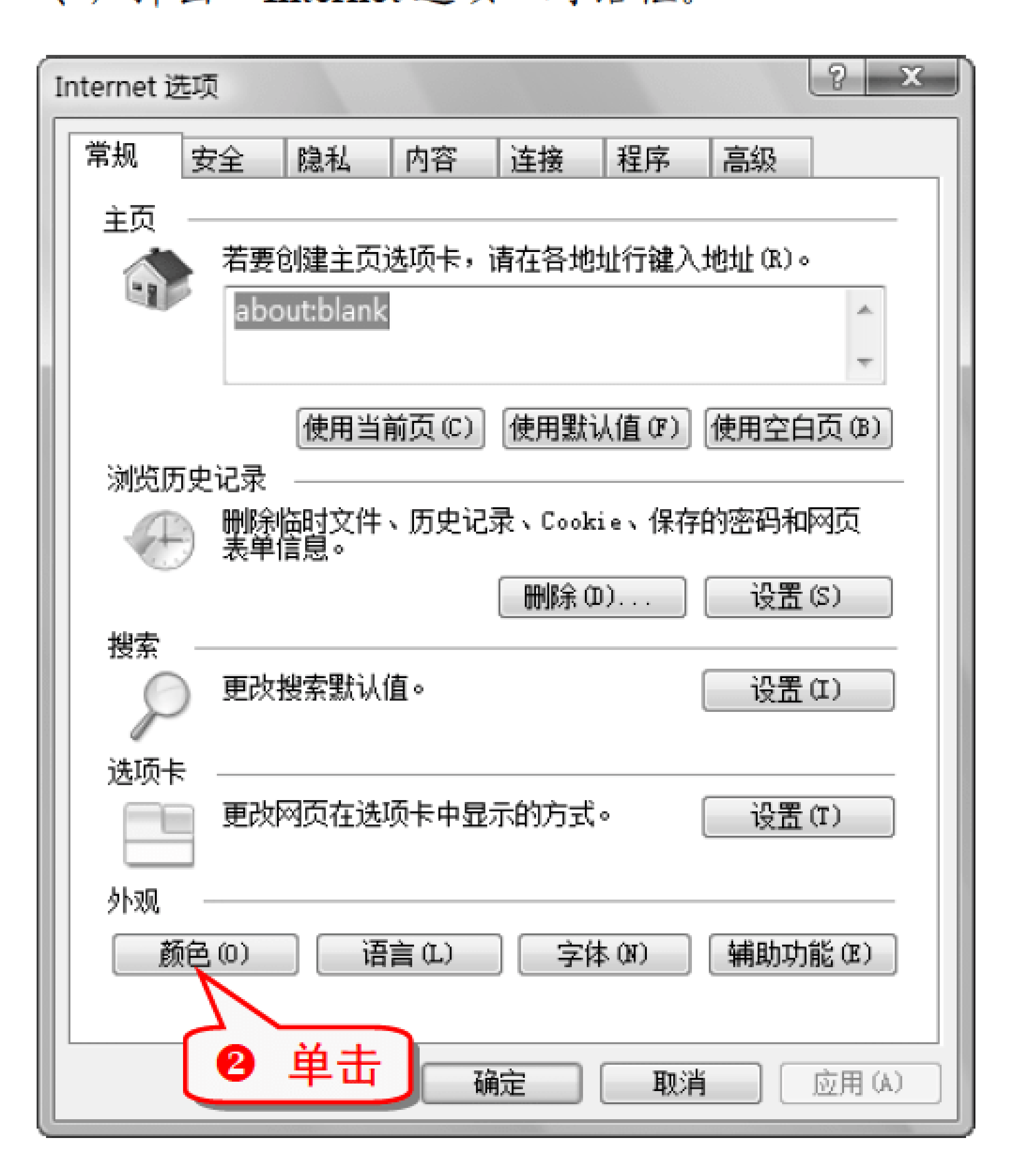
❶ 打开 IE 浏览器，按下 Ctrl + Shift + I 组合键。



技巧20 消除已访问 IE 地址的颜色变化

使用 IE 上网时，会碰到已访问过的链接变成不同的颜色的情况。虽然这方便了浏览，但会不经意间泄露用户的浏览痕迹。

❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框。

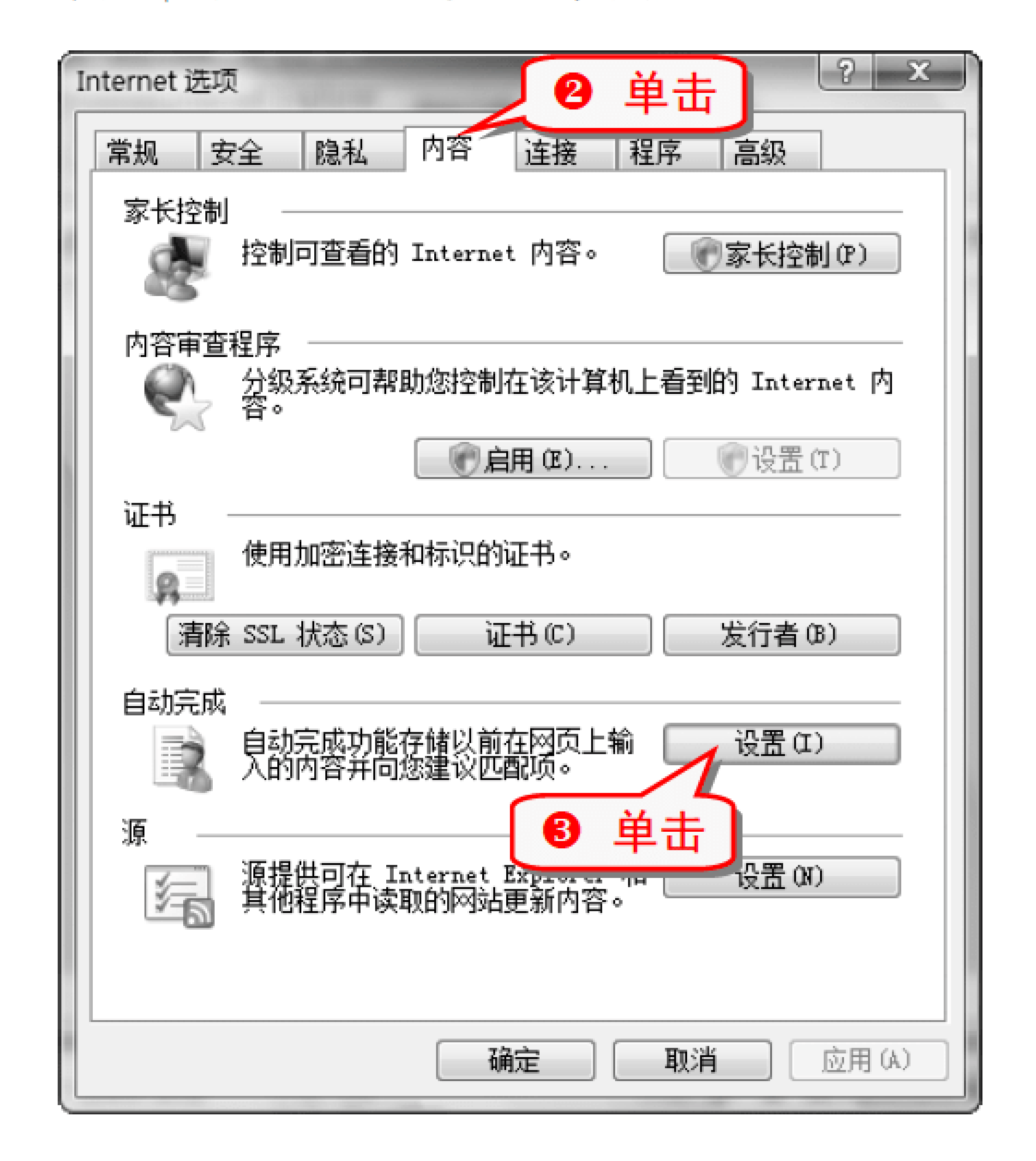




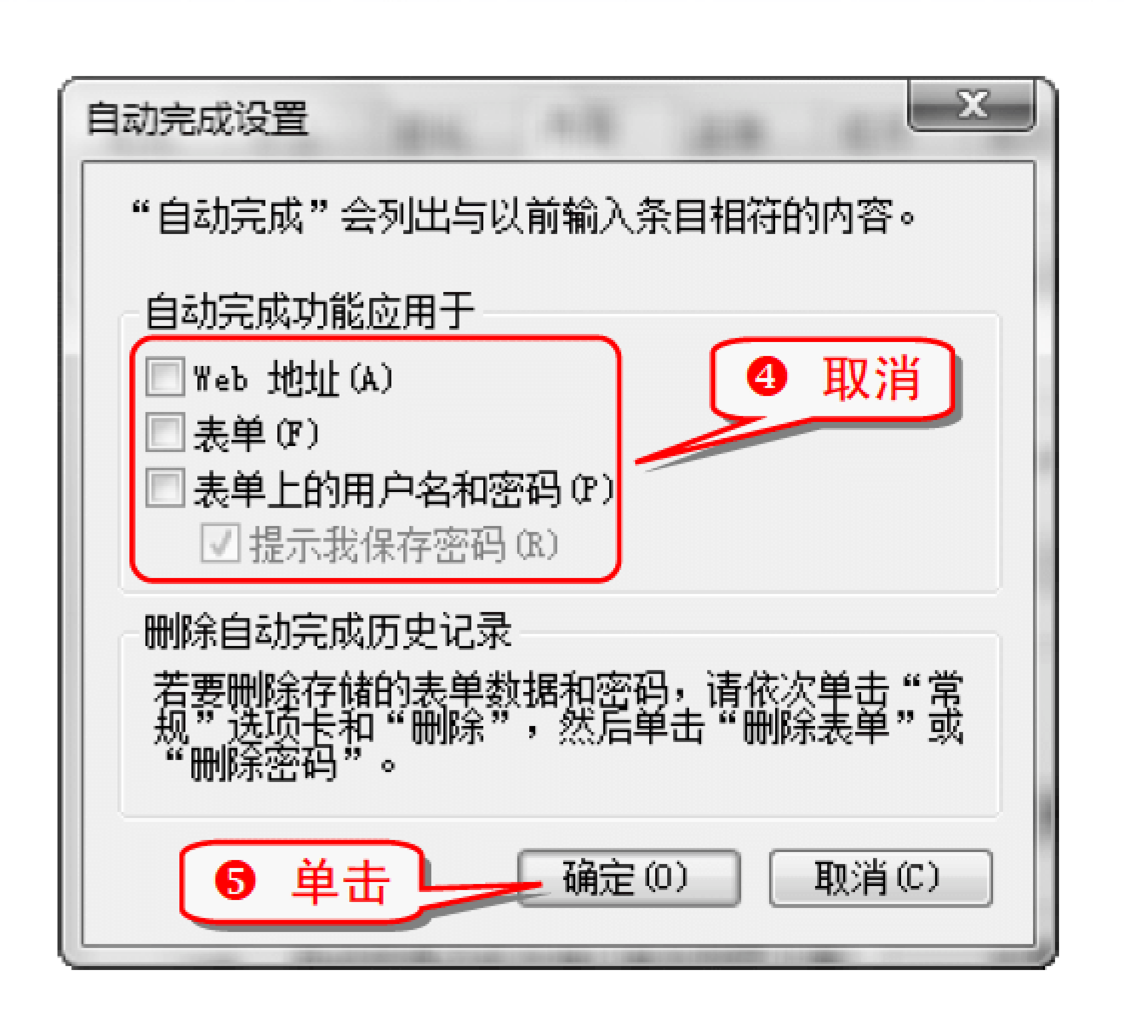
技巧21 使 IE 不再自动填写表单

IE 中的自动完成功能给填写表单带来一定的便利，同时也带来了潜在的危险，尤其是对于在网吧或公共场所上网的网民。为了安全可以禁止该功能。

❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框。



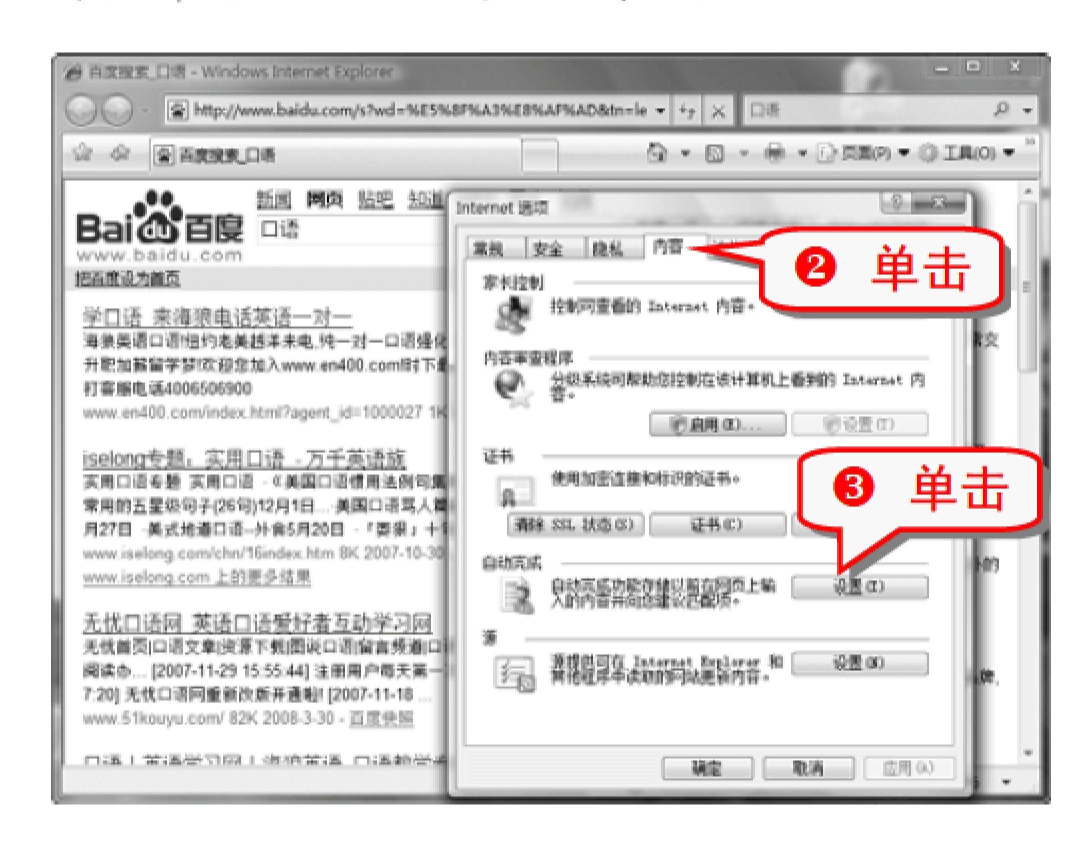


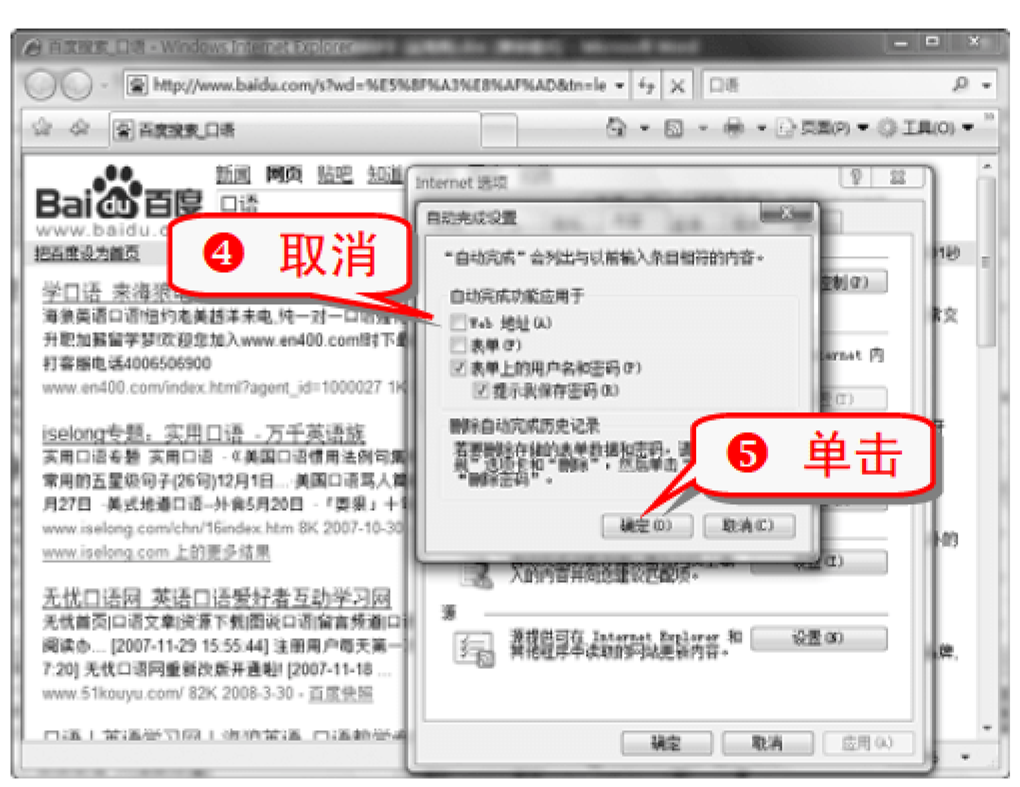


技巧22　清除 IE 地址栏的自动匹配功能

在 IE 浏览器的地址栏内，当输入要访问的网站地址的部分字母时，地址栏中会自动打开一个列表，列出最近访问过的与输入字母相匹配的站点地址，如果不想出现这种情况，可以采用以下步骤取消自动匹配功能。

❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框。





技巧23　使输入的网址不被 IE 记录

IE 浏览器会记录最近输入的每个网址，通过地址栏的下拉列表可以看到最近输入的网址。通过以下步骤访问网页，所输入的网址将不会被记录。

❶ 打开 IE 浏览器，按下 Ctrl + O 组合键。

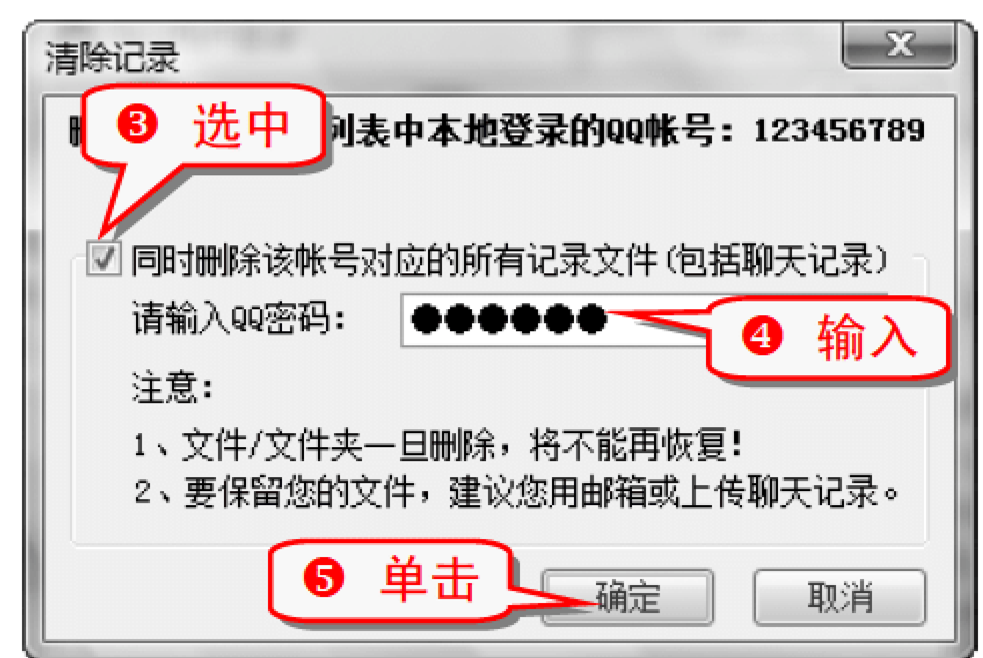


技巧24　快速清除 QQ 使用记录

QQ 会自动记录登录号码和聊天记录，很多秘密被记录在电脑里面，及时清除 QQ 的使用记录，能保证 QQ 聊天的隐私安全。

❶ 打开 QQ 2008 的登录对话框。

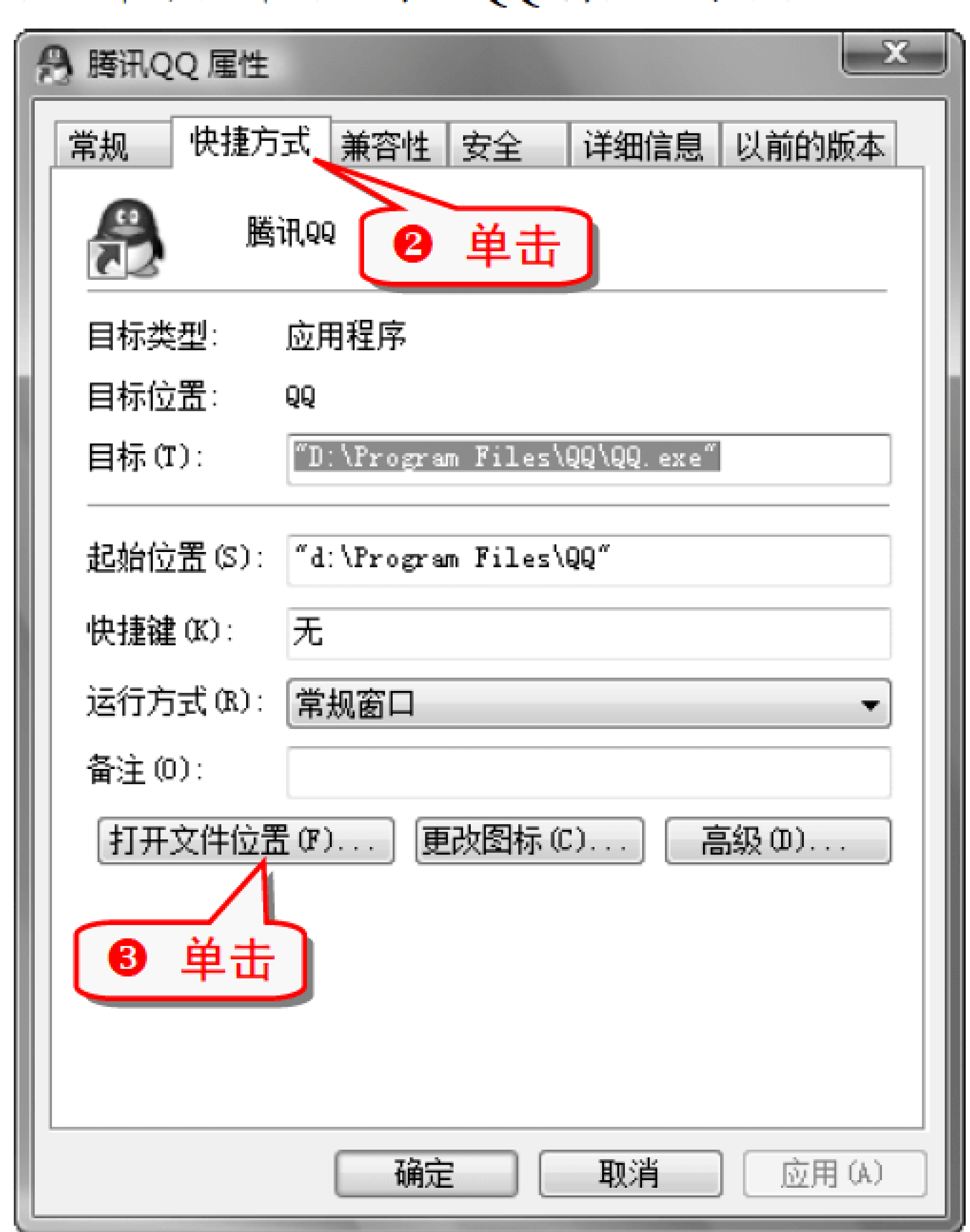




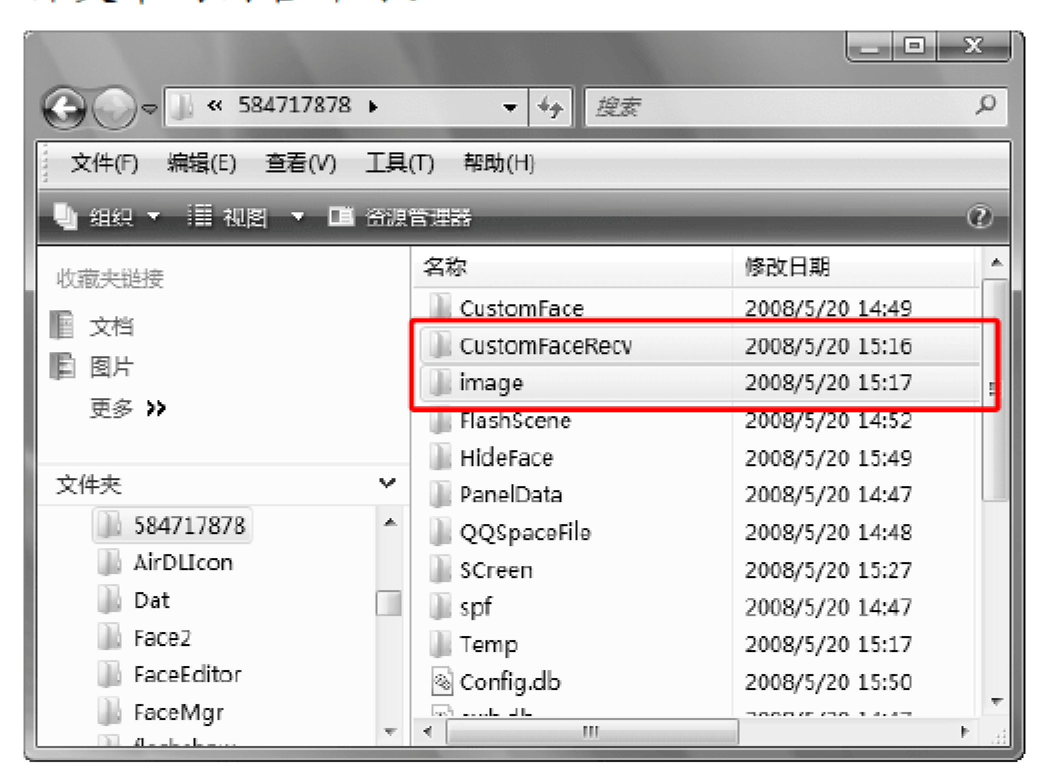
技巧25 定期清理 QQ 无用文件夹

QQ 使用久了，所占用的磁盘空间也会越来越大，将一些无用的文件删除，可以释放一些磁盘空间并且保证隐私安全。

❶ 右击桌面上的 QQ 图标，在弹出的快捷菜单中选择“属性”命令，弹出“腾讯 QQ 属性”对话框。



❹ 打开 QQ 的安装目录，在每个 QQ 号码的文件夹中找到 CustomFaceRecv 文件夹和 image 文件夹，并删除文件夹中的内容即可。



专 家 坐 堂

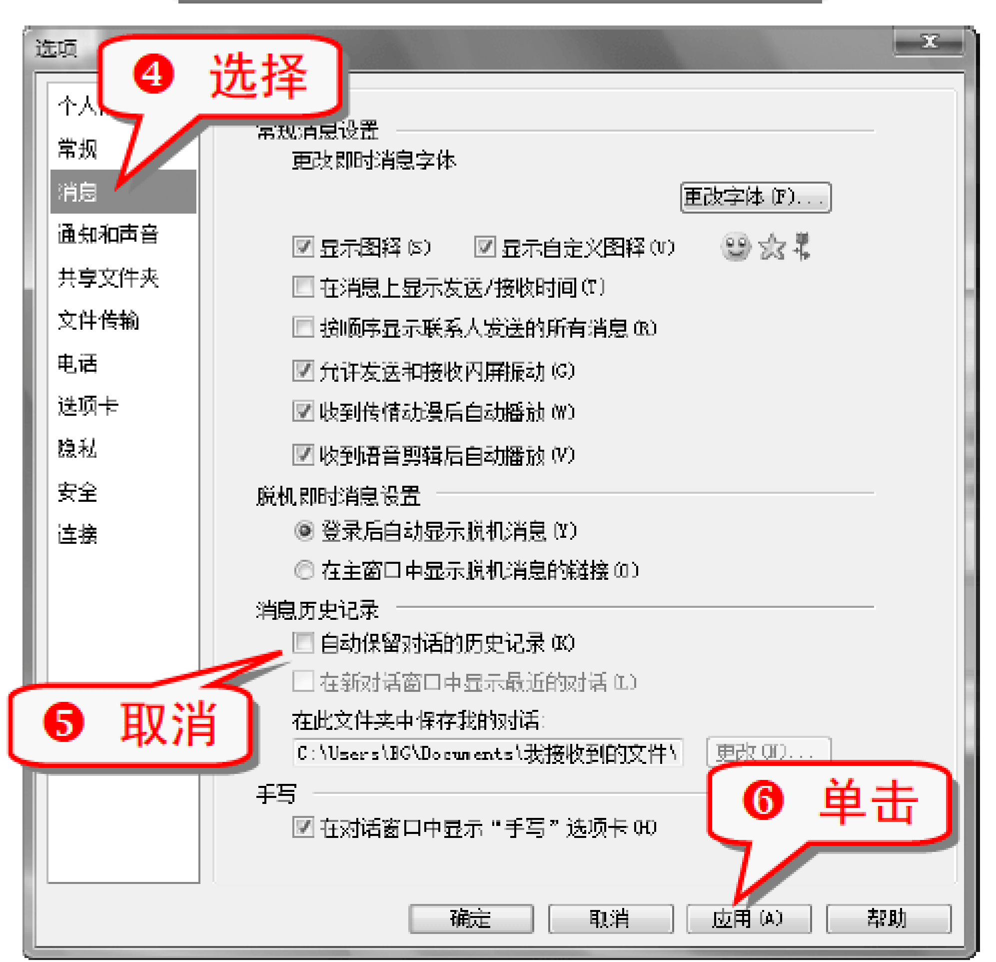
这两个文件夹是 QQ 的图片缓存目录，聊天时发送的表情、截图以及 QQ 群中发送的图片，都会保存在这里。时间一久，这两个文件夹的容量会越来越大。

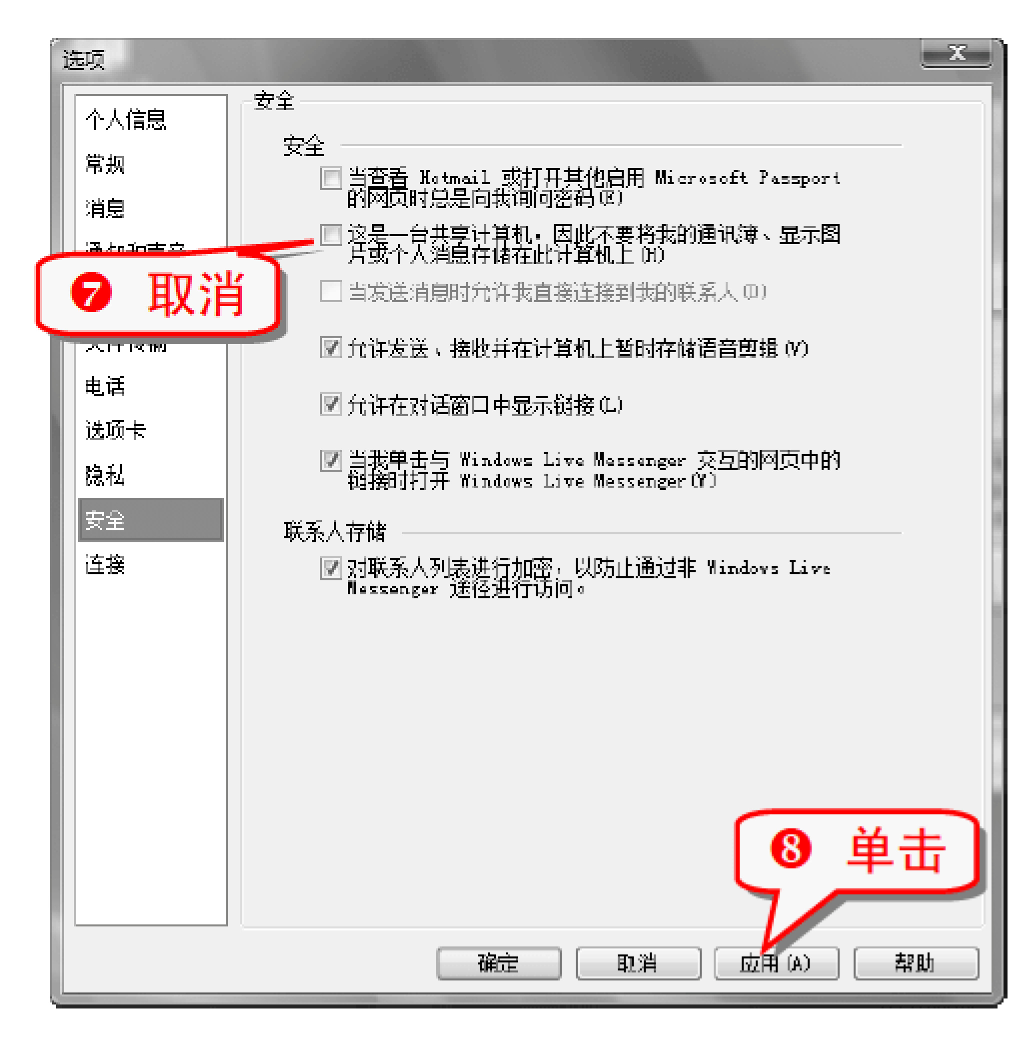
技巧26 使 MSN 不保留历史记录

在 MSN Messenger 中登录后，通过简单的几步设置，就可以让 MSN 不保留历史记录。

❶ 打开 MSN 的登录对话框。









技巧27　清除迅雷的下载记录

迅雷是比较流行的下载工具，以速度快而赢得很多用户的青睐，但是会留下许多操作痕迹。要及时删除这些下载记录。

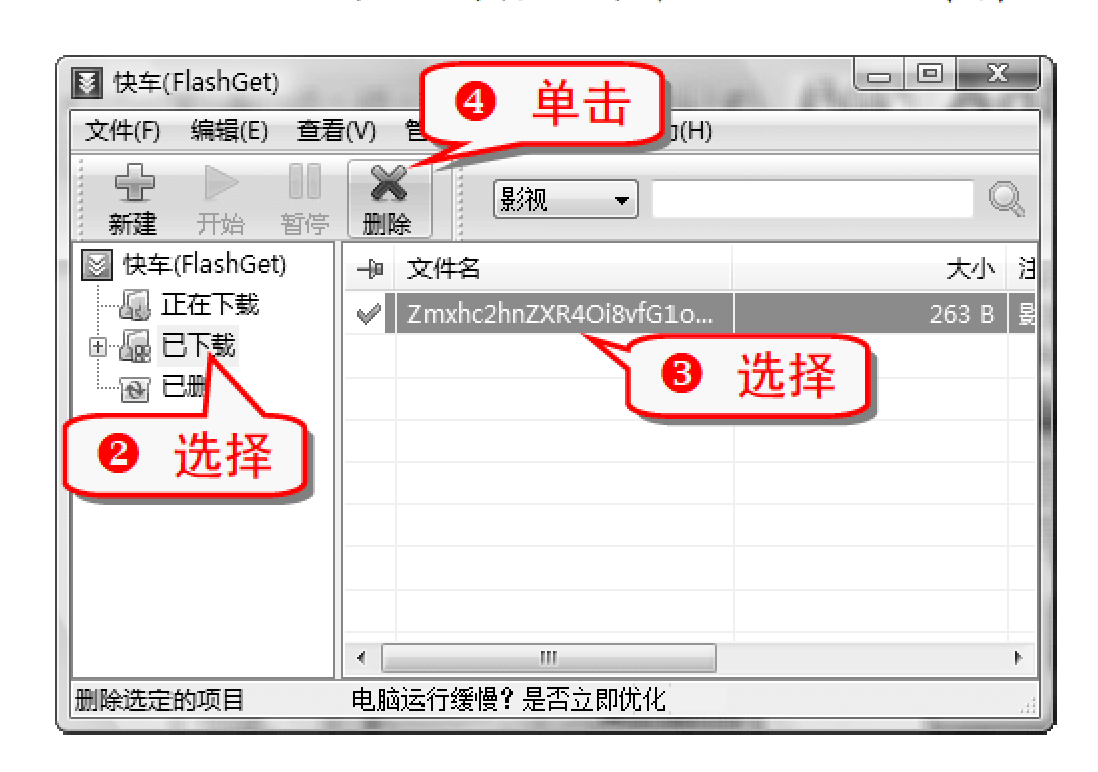
❶ 双击迅雷快捷图标，打开迅雷工作窗口。

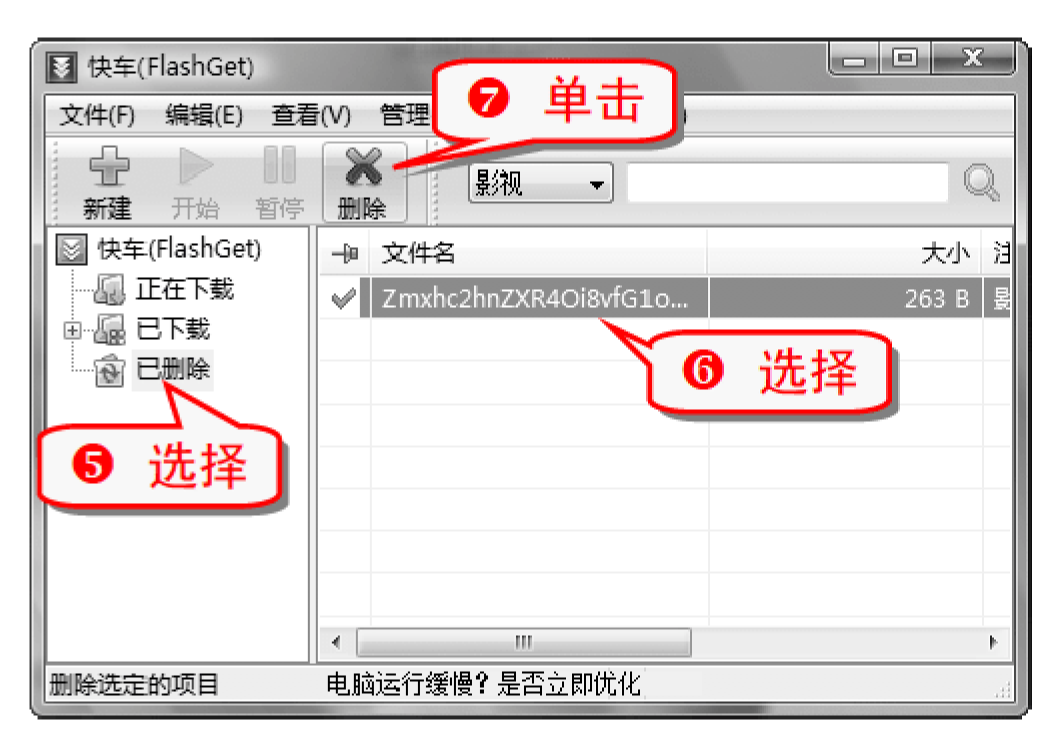


技巧28　清除 FlashGet 的下载记录

FlashGet(网际快车)作为一款国产的精品下载软件，也会保留曾经下载过的文件目录。执行“文件”→“最近下载的文件”命令，或在打开 FlashGet 时按下 Ctrl+R 组合键，即可出现全部下载记录。

❶ 双击 FlashGet 快捷图标，打开 FlashGet 工作窗口。



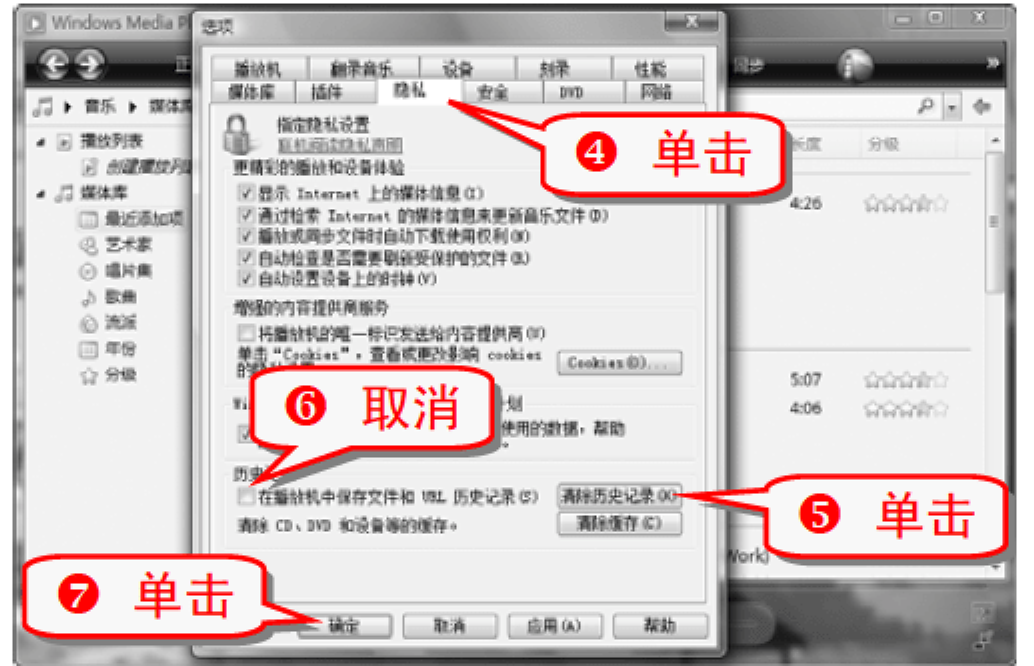


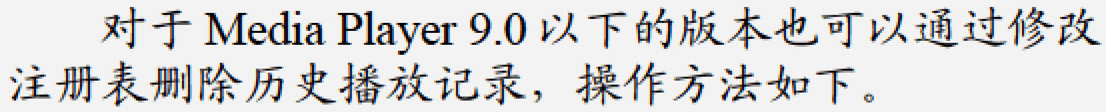
技巧29　清除 Media Player 播放记录

使用 Media Player 对多媒体文件进行播放的过程中，会自动记录最近几次的播放记录以及这些多媒体文件的播放路径，这就暴露了个人隐私，应该将其清除。

❶ 打开 Media Player 播放器。







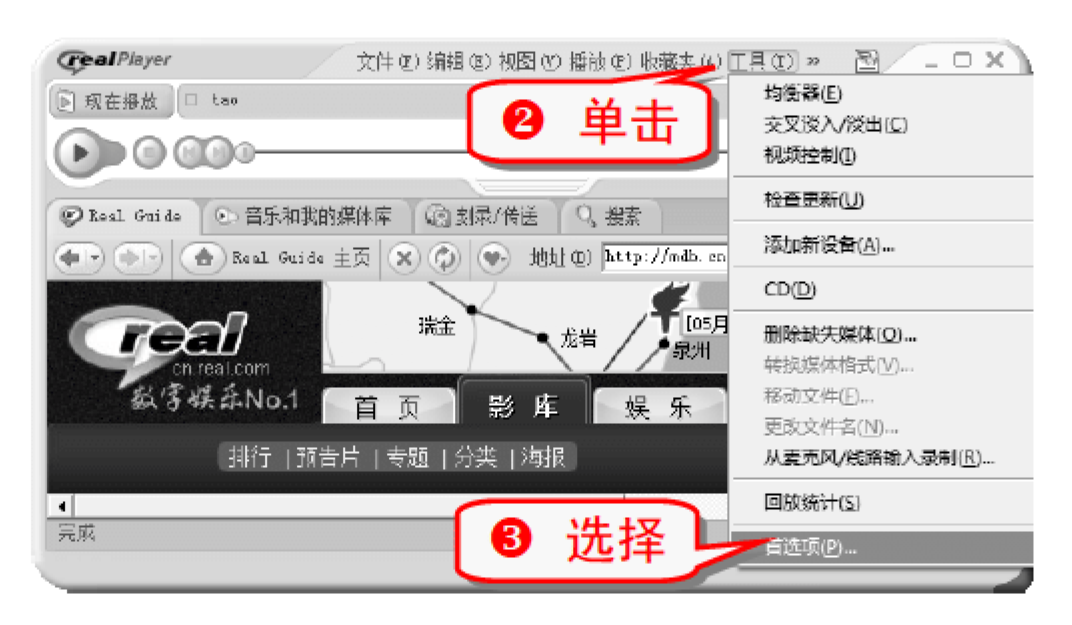
对于 Media Player 9.0 以下的版本也可以通过修改注册表删除历史播放记录，操作方法如下。

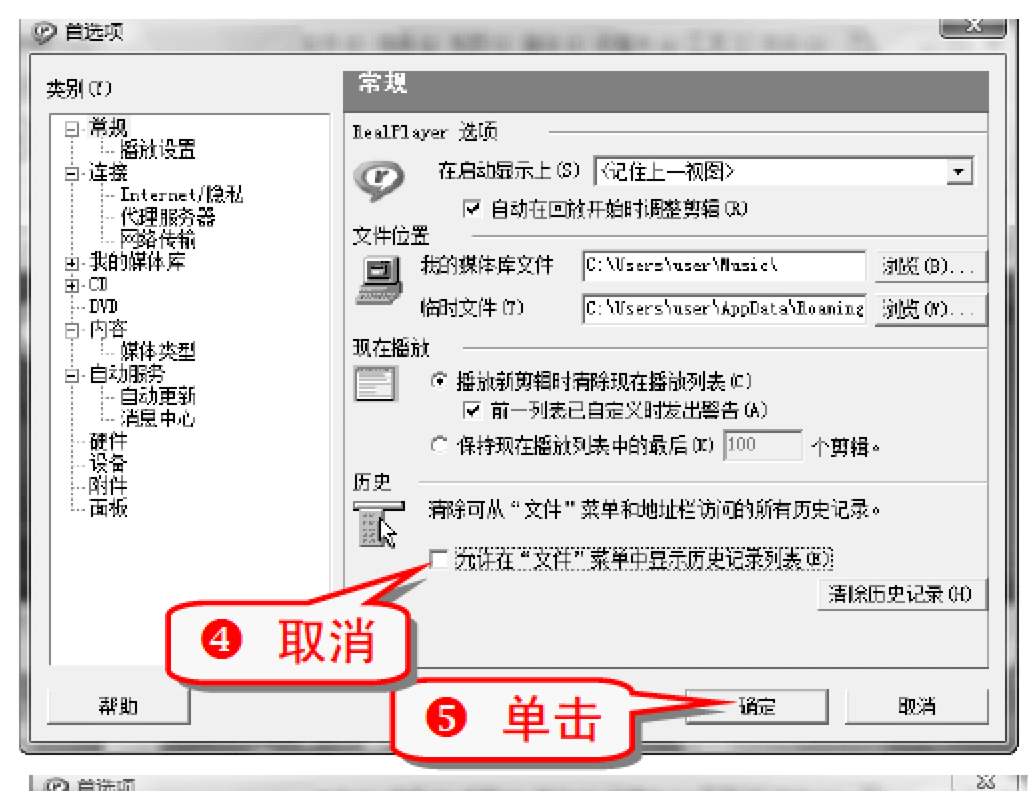
打开注册表编辑器，展开 HKEY_CURRENT_USER/Software/Microsoft/MediaPlayer/Player/RecentFileList 分支，在右边的窗格中，就列有 URL0、URL1、URL2 等播放记录，把这些键值全部删除，即可将播放记录清除干净。

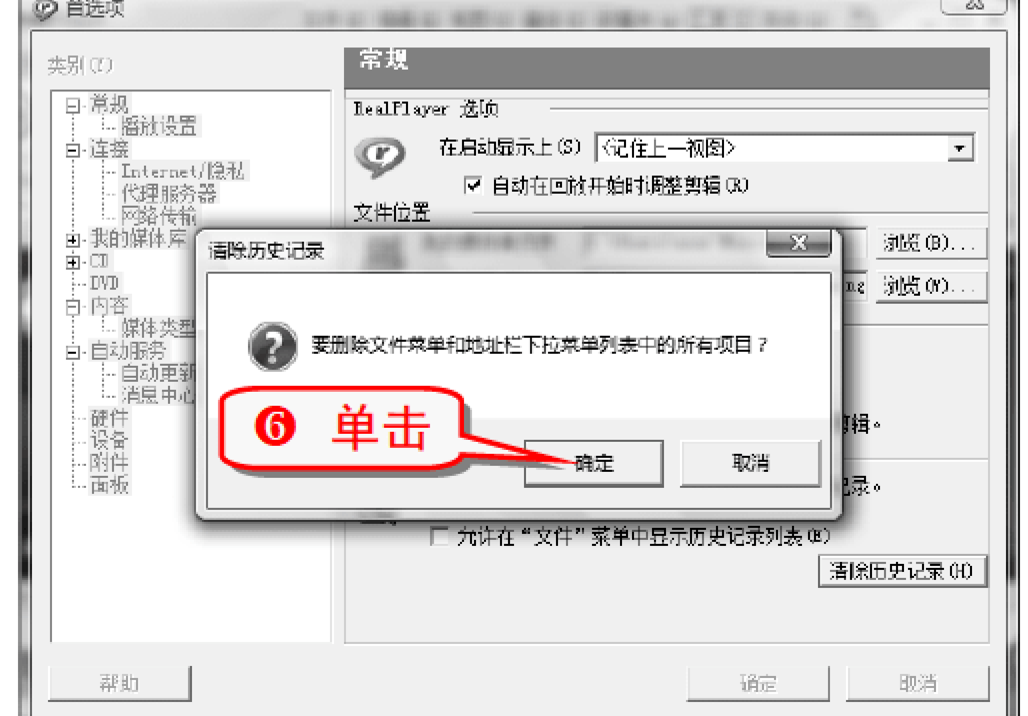
技巧30　清除 RealPlayer 播放记录

如果经常使用 RealPlayer 可以发现，在该软件的文件菜单中保存了最近打开的一些文件记录。可以通过以下方法进行删除，并让其不再显示最近打开过的文件记录。

❶ 打开 RealPlayer 播放器。







举 一 反 三

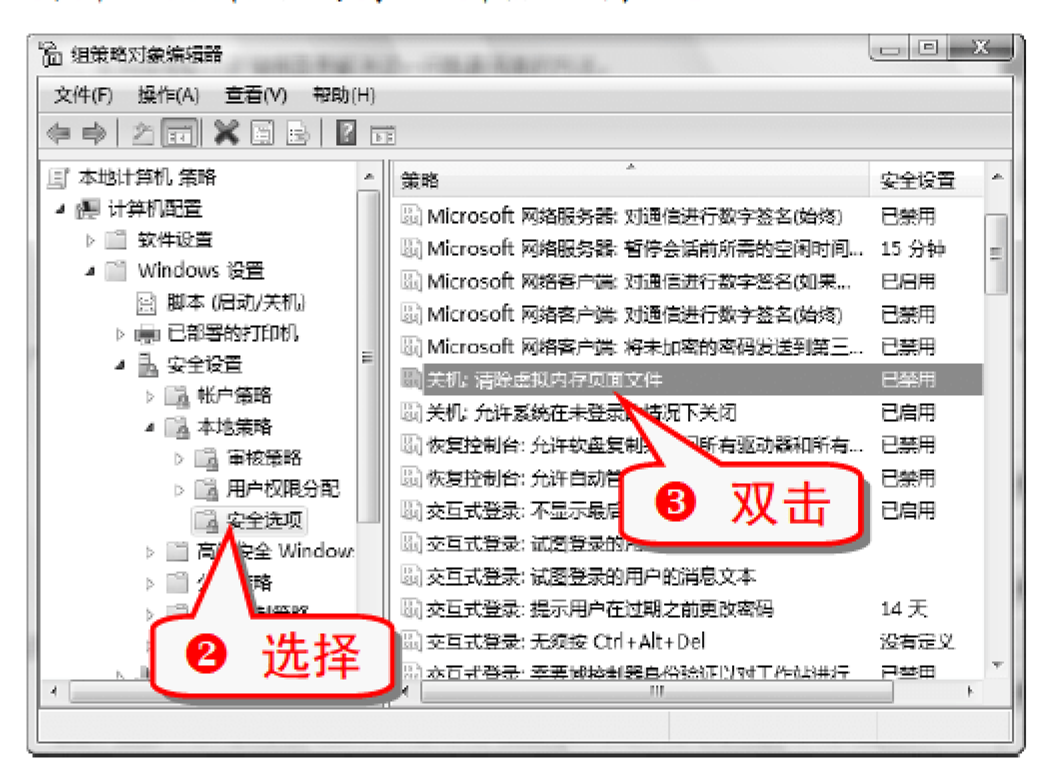
通过修改注册表也可以删除 RealPlayer 播放记录，操作方法如下。

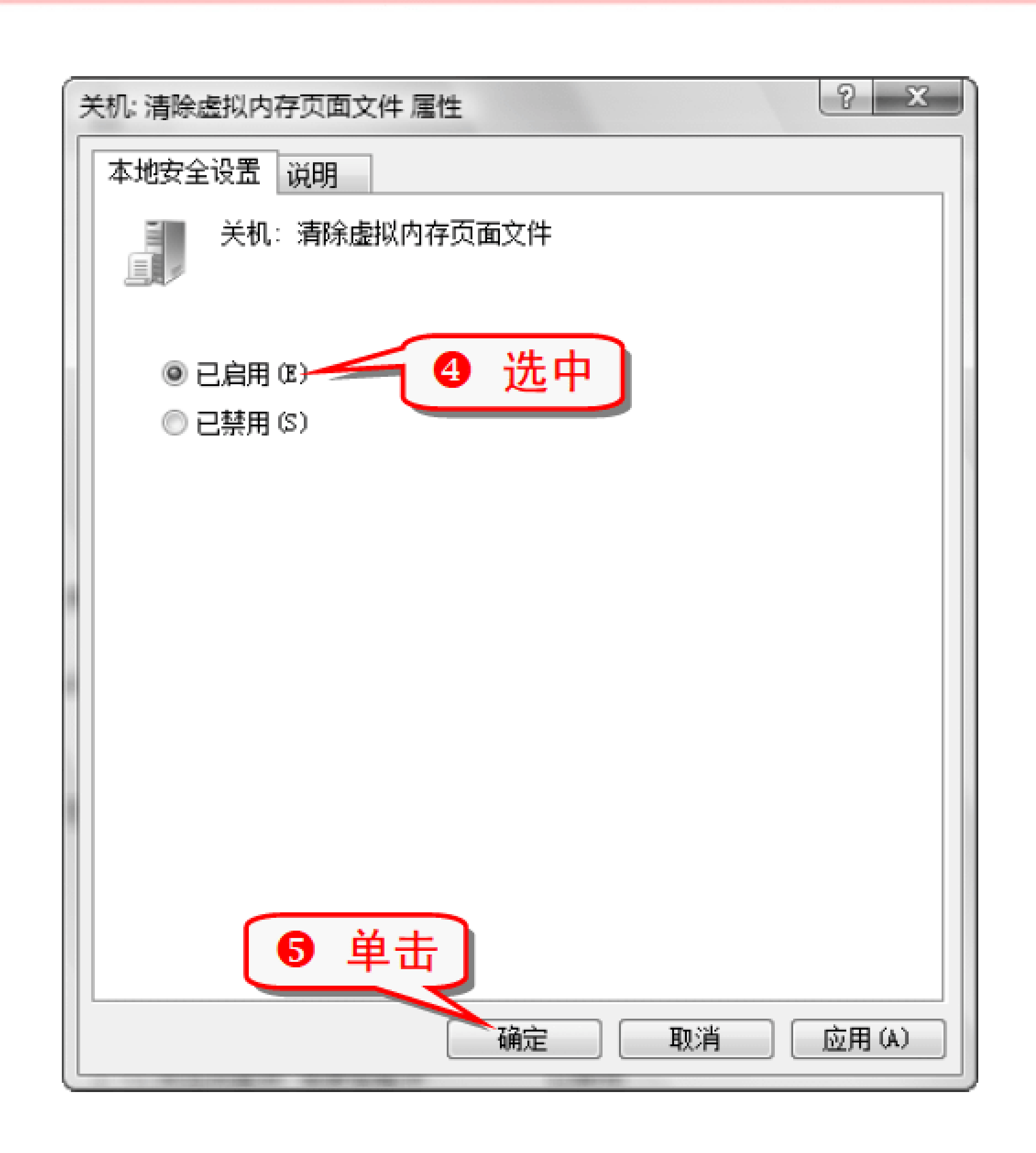
打开注册表编辑器，展开 HKEY_CURRENT_USER/Software/RealNetworks/RealPlayer/8.0/Preferences 分支，在该分支下找到多个 Most RecentClips 主键，在该主键下找到最近打开的文件地址，将其删除即可。

技巧31 关机时自动清除页面文件

页面文件中含有一些敏感的个人资料，为了避免泄露这些资料，可以设置系统在关闭时自动删除页面文件。

❶ 打开“组策略对象编辑器”窗口。

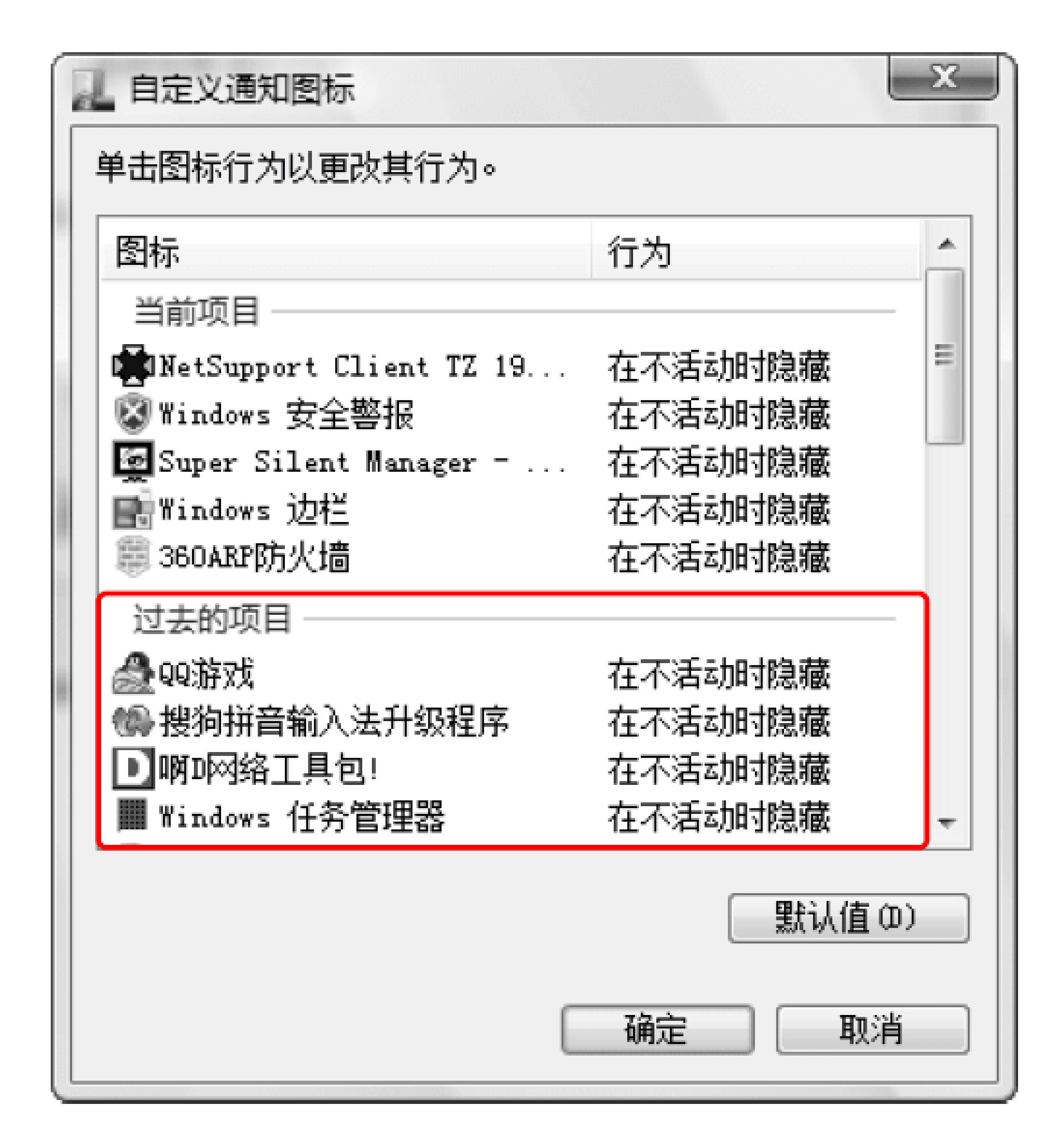




技巧32 清除托盘区不使用的图标记录

Windows Vista 中有“隐藏不活动的图标”这个功能，会产生系统托盘图标的历史记录。

右击通知区域的16:31图标，在弹出的快捷菜单中选择“自定义通知图标”命令，弹出“自定义通知图标”对话框。

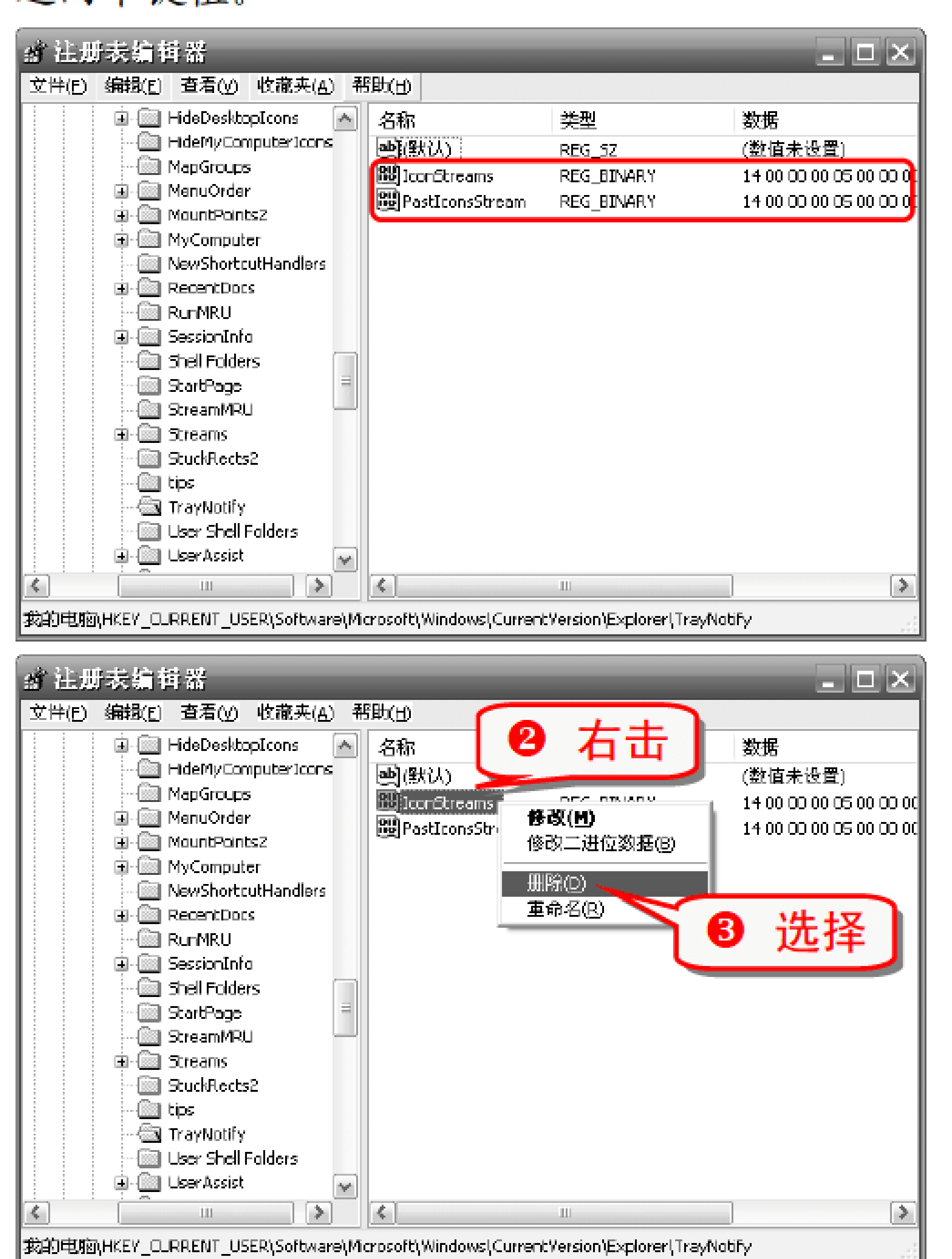


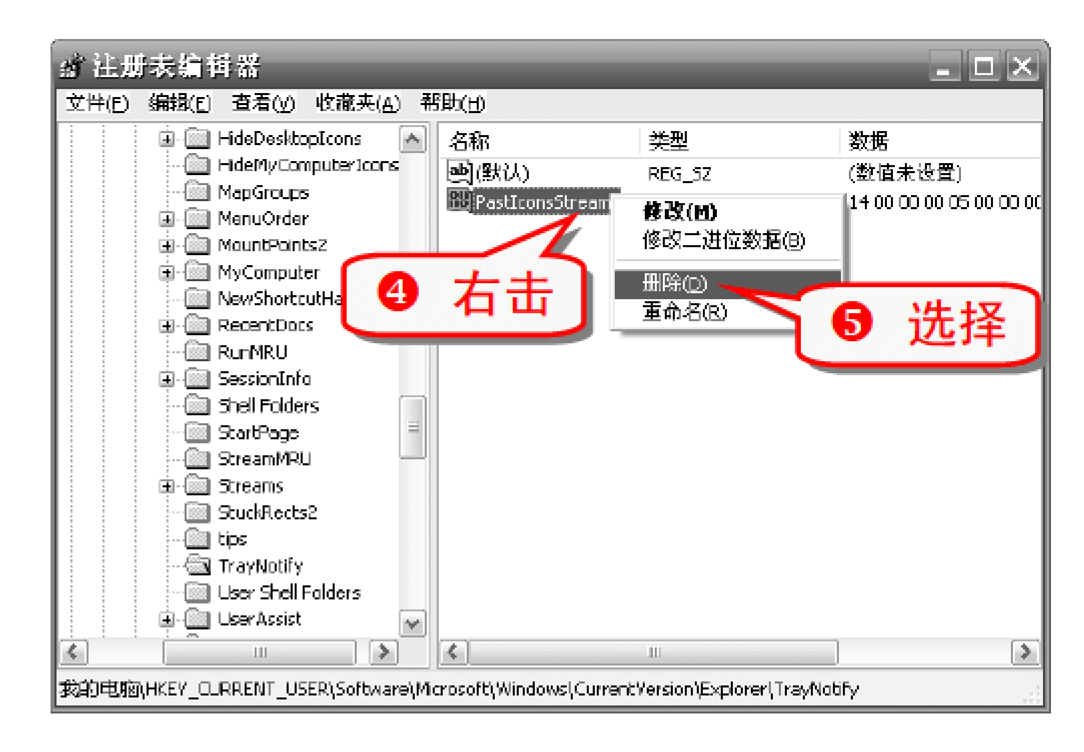
在“过去的项目”选项组中可以发现以前运行过的一些程序图标，即使这些程序已经删除，图标仍被记录在案。为了防止“过去的项目”泄露隐私，有必要将其删除。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\



TrayNotify 分支，找到 IconStreams 和 PastIconsStream 这两个键值。



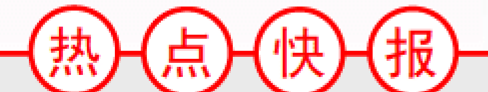




专题二　将隐藏进行到底

内容导航

电脑中存放着很多重要的隐私文件，如果被黑客窃取，会造成很大的损失。养成隐藏重要文件的习惯，可以很好地保护个人隐私，而且隐藏电脑的重要功能可以有效地防止黑客入侵。

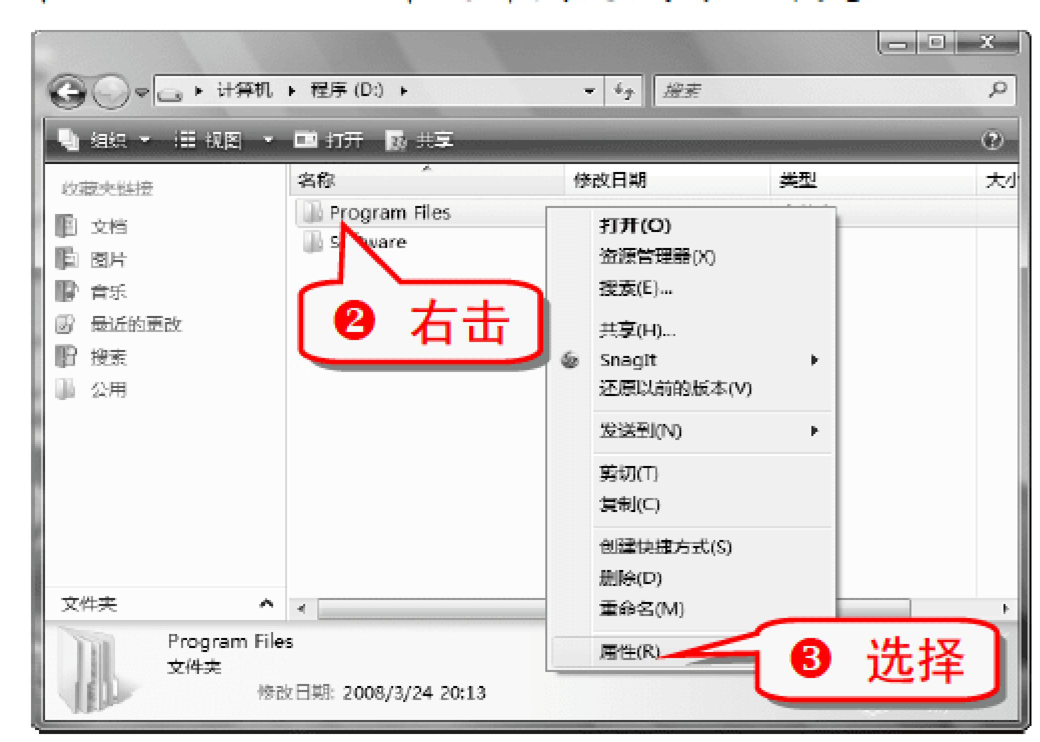


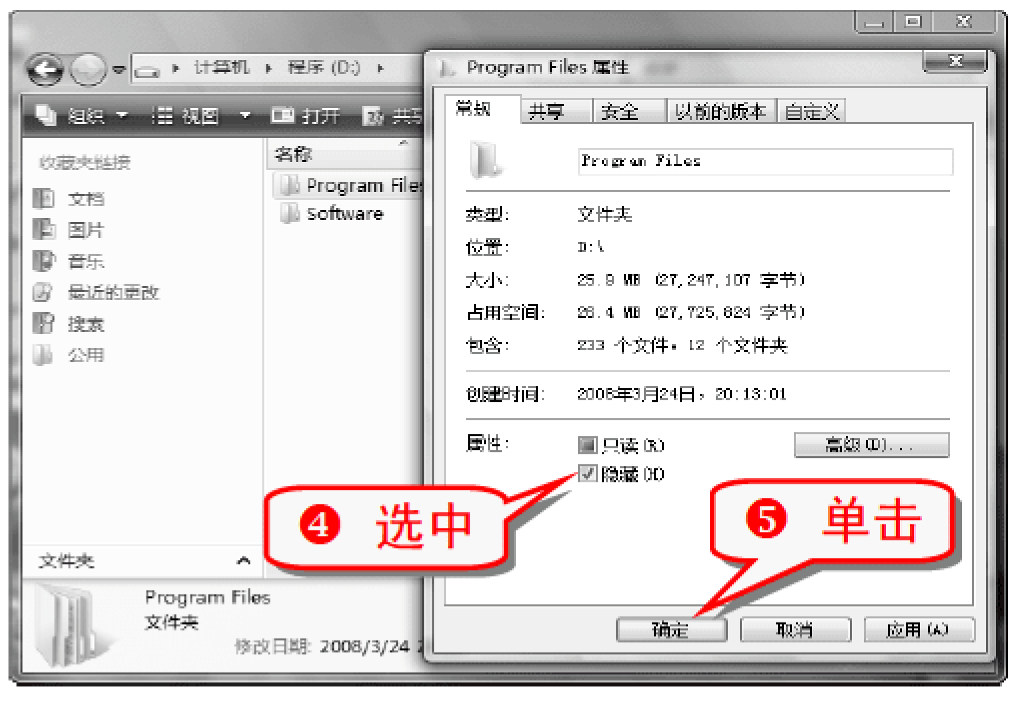
- 文件夹隐藏技巧
- 给文件改头换面
- 隐藏电脑驱动器
- 隐藏桌面回收站
- 隐藏网上邻居
- 隐藏 QQ 的 IP 地址

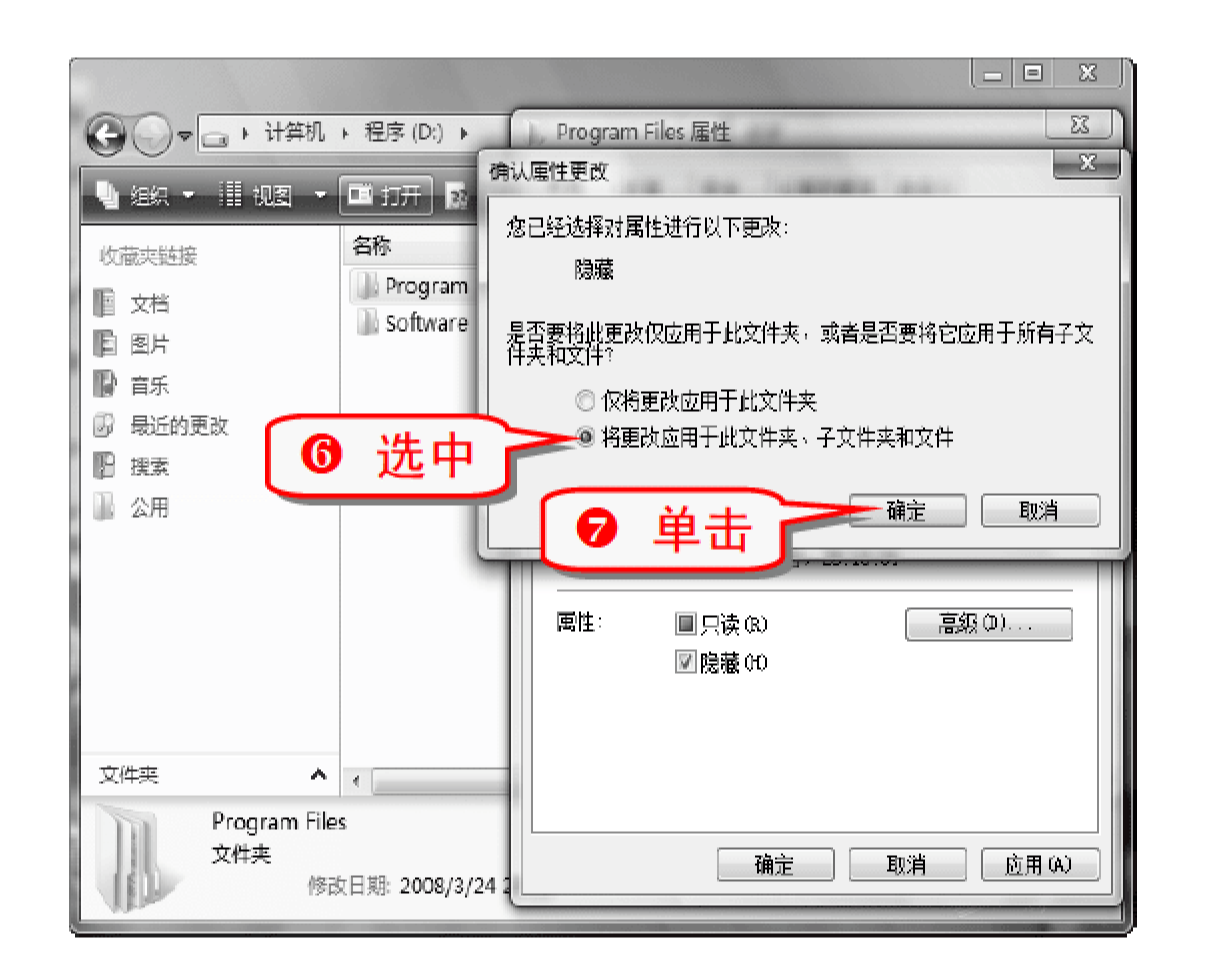
技巧33　隐藏文件夹

很多文件涉及个人隐私，因而不希望别人看到，可以通过隐藏文件夹的方式将其文件属性设置为“隐藏”，达到保护隐私的目的。

❶ 在 Windows Vista 中选择要隐藏的文件夹。







注　意　事　项

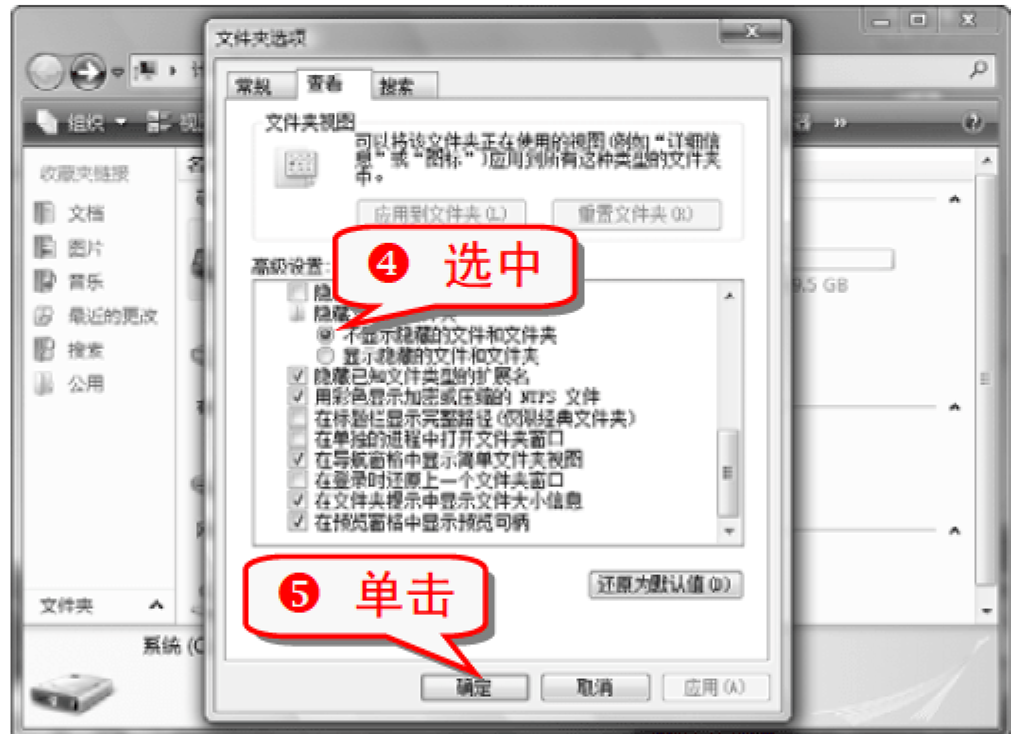
上述步骤只能达到隐藏文件的效果，要让隐藏的文件不显示，需要进行进一步的设置。

技巧34　使隐藏的文件夹不显示

将文件夹设置为隐藏之后，通过简单的几步设置可以让隐藏的文件夹从系统中“消失”。

❶ 双击桌面上的“计算机”图标，打开计算机的窗口。



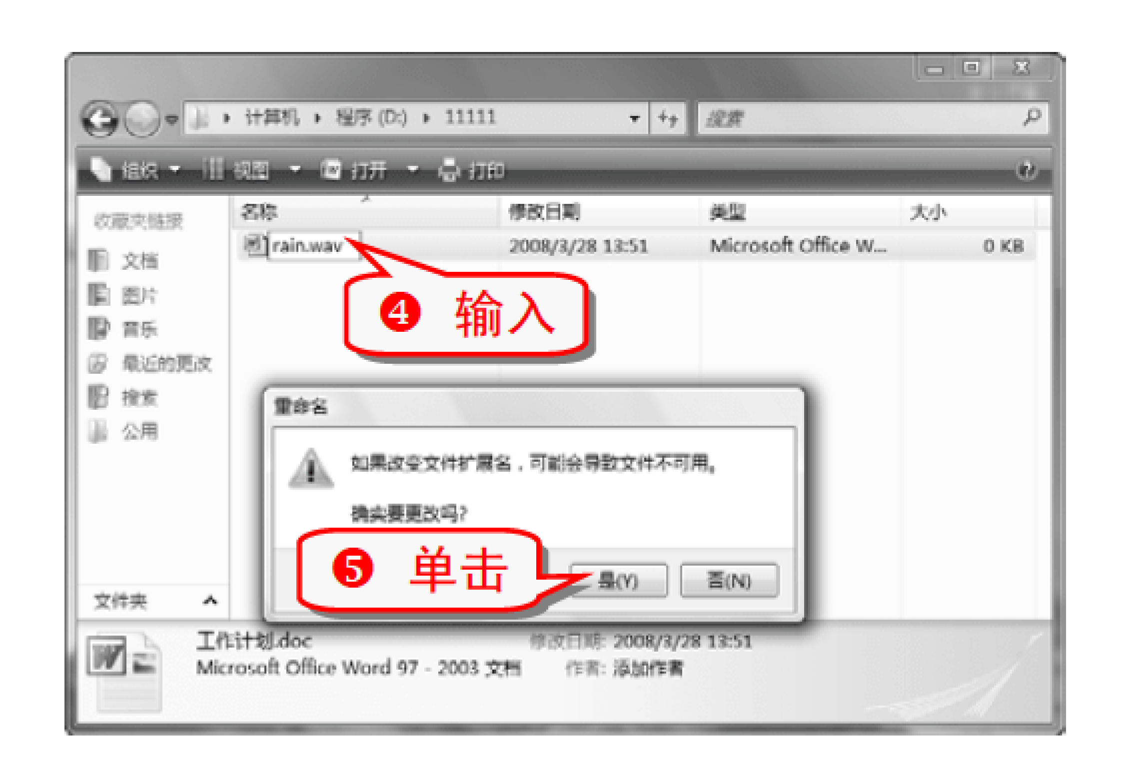


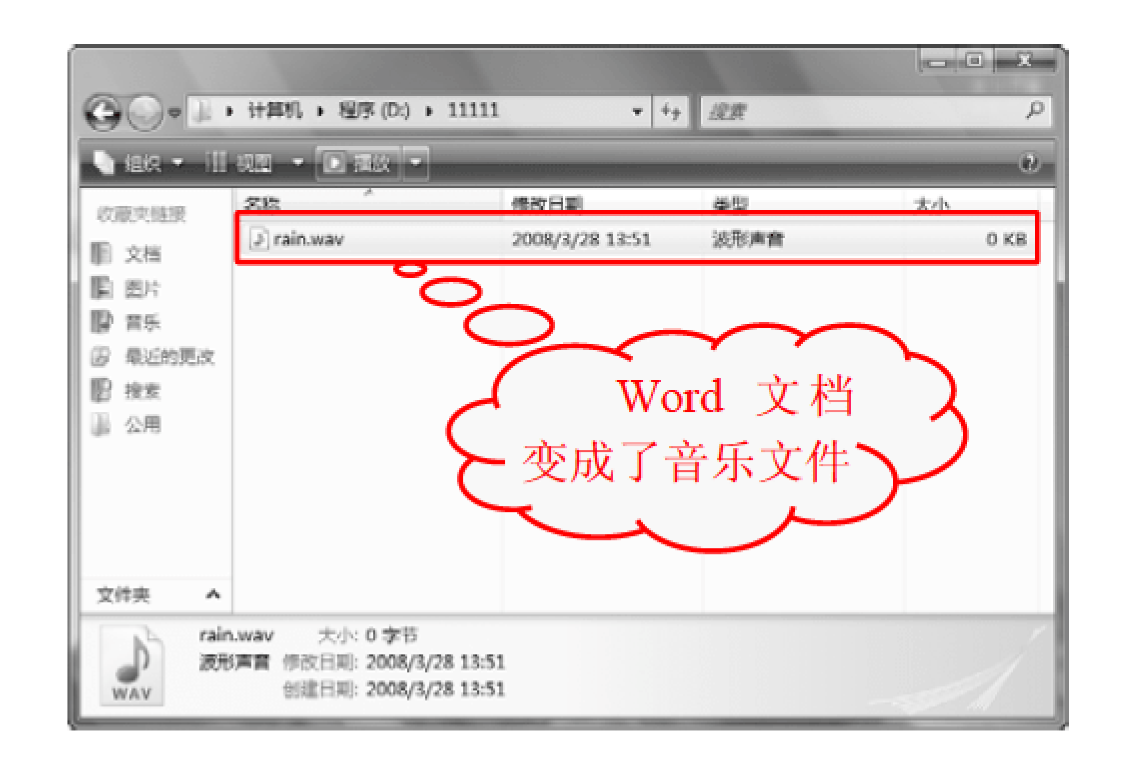
技巧35 更改后缀名以隐藏文件

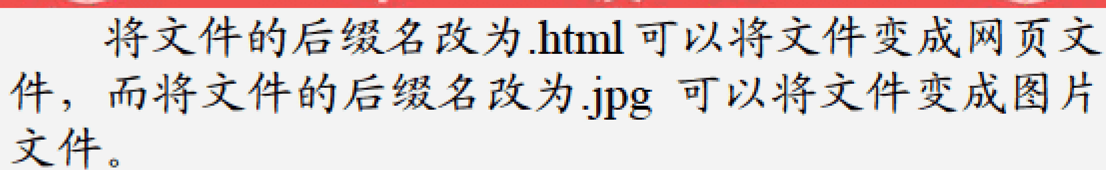
隐藏文件能做到加密的效果，更改文件的后缀名也能起到加密的效果。

❶ 在 Windows Vista 中选择要更改后缀名的文件。









将文件的后缀名改为.html 可以将文件变成网页文件，而将文件的后缀名改为.jpg 可以将文件变成图片文件。

注 意 事 项

对于更改过后缀名的重要文件，要将其放到特定的文件目录下，防止被误删。

技巧36 巧改文件名隐藏文件

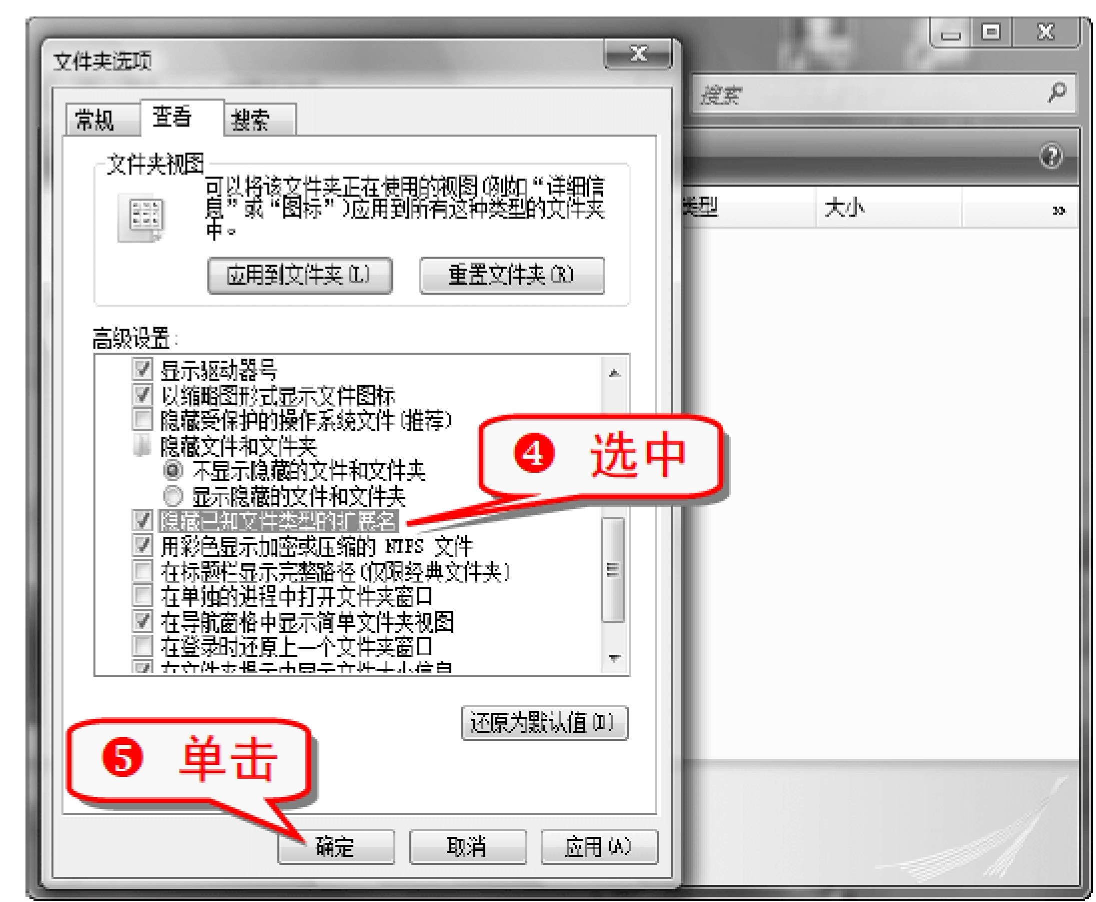
文件的后缀名在电脑中是可以被隐藏的，隐藏原有的后缀名以后，再给文件名后面多加一个后缀名，并且修改默认的打开方式，就可以将重要的文件很好地藏起来。

(1) 将文件的真实后缀名隐藏

❶ 在 Windows Vista 系统中打开放有重要文件的文件夹。







(2) 给文件加一个伪装的后缀名

❶ 右击要伪装的 Word 文档，在弹出的快捷菜单中选择“重命名”命令。







注　意　事　项

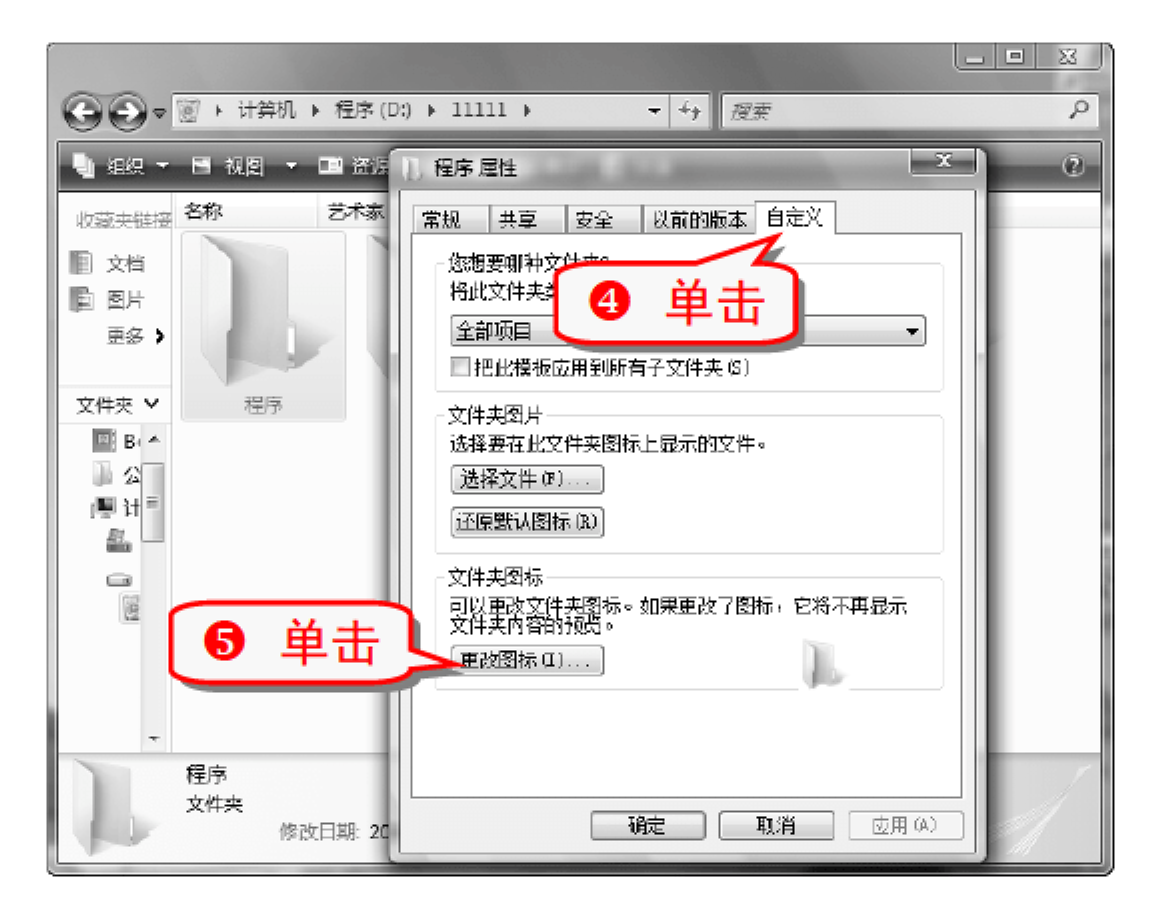
这样做有一点不利之处，同种文件都会用这种方式打开。最好的方法是将文件的图标给替换掉。

技巧37　将私人文件夹变为回收站

将重要文件夹的图标变成回收站的图标，会带来一个视觉误导，达到加密的效果。

❶ 在 Windows Vista 系统中选择要更改的文件夹。









注 意 事 项

可以将更改为回收站图标的文件夹中的内容进行加密和隐藏，这样就可以完美地将重要的文件隐藏起来。

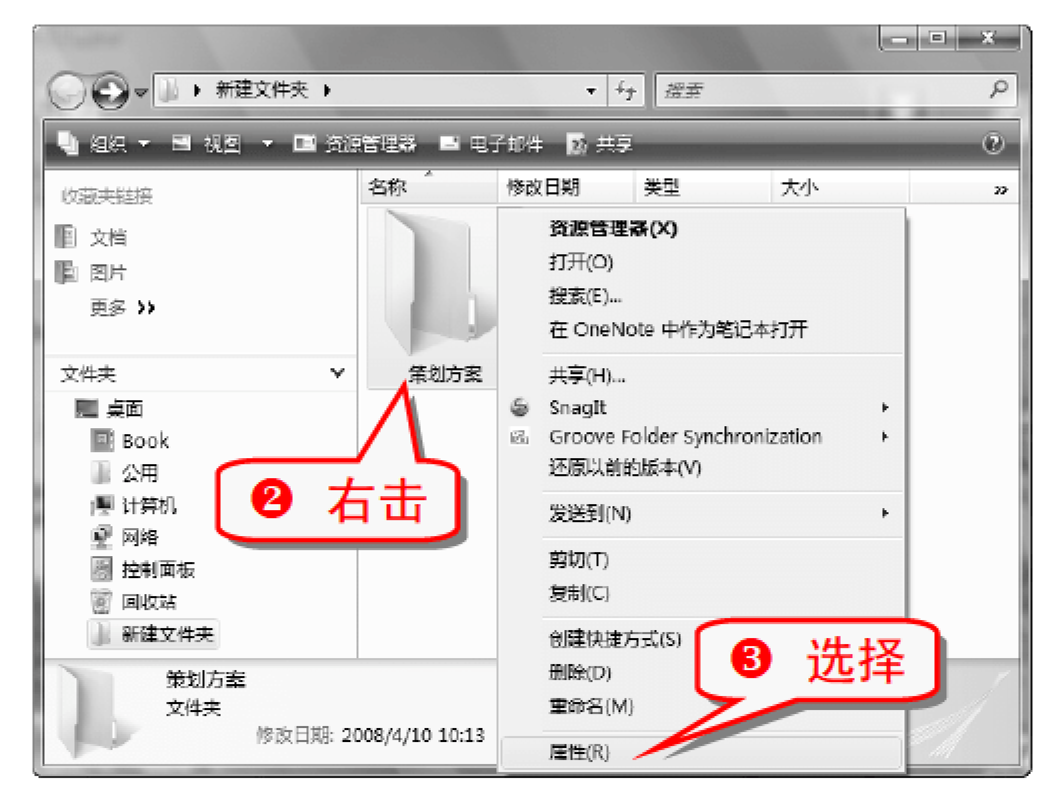
举 一 反 三

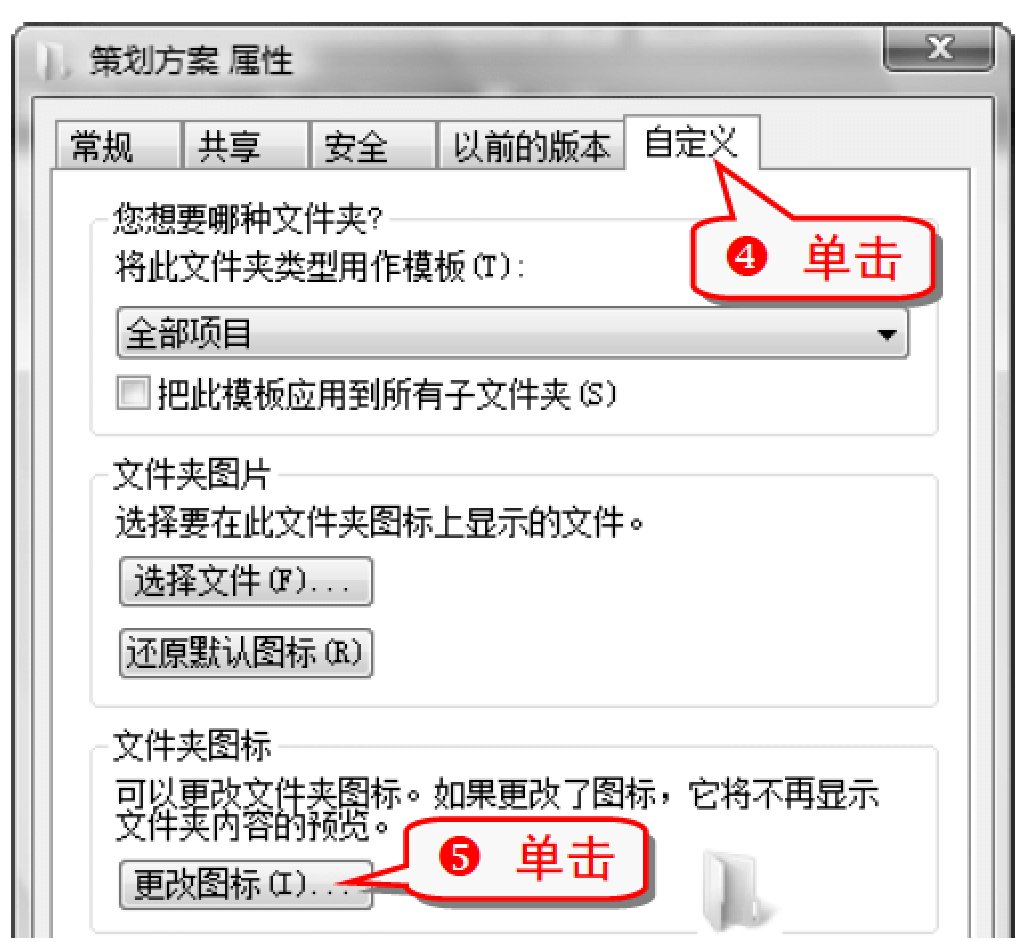
通过类似的方法可以将私人文件夹伪装成网上邻居、浏览器、驱动器以及移动硬盘等。

技巧38　将私人文件夹变为系统文件

系统文件是电脑中最重要的文件，改变系统文件稍有不慎就可能破坏系统。如果将私人文件夹伪装成系统文件，不失为一个绝好的隐藏方法。

❶ 在 Windows Vista 系统中选择要伪装成系统文件的文件夹。

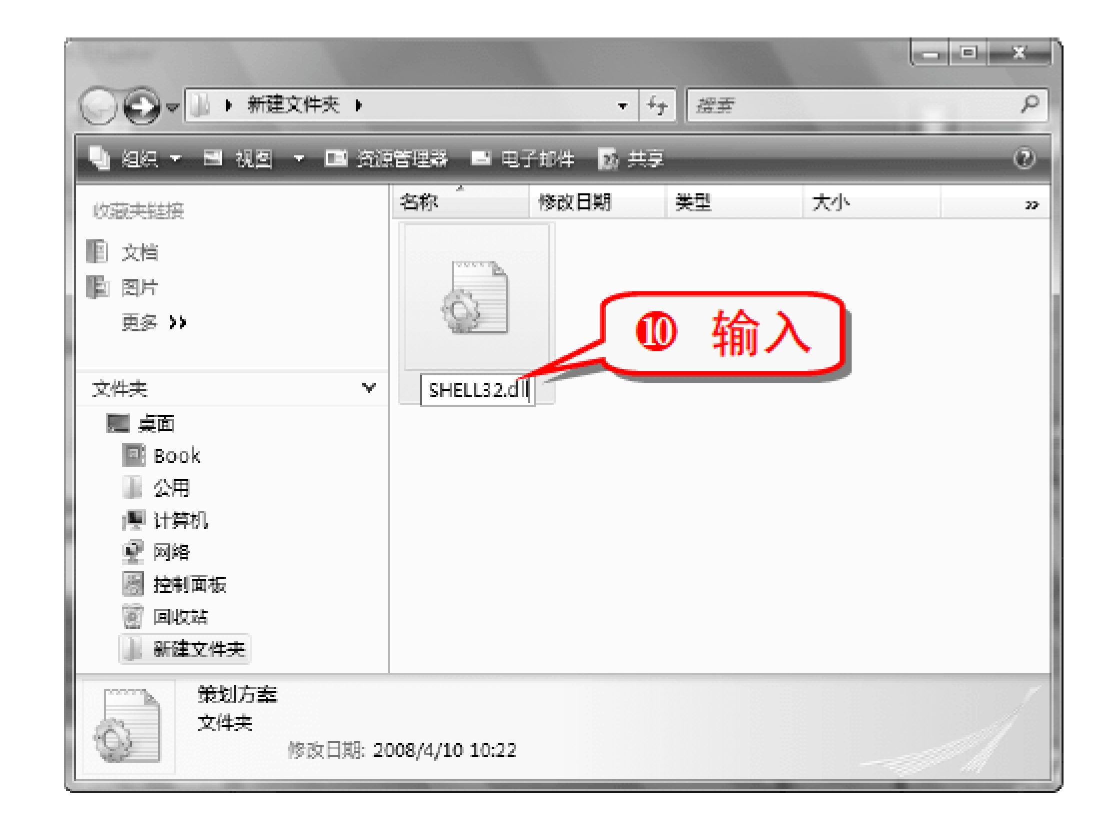










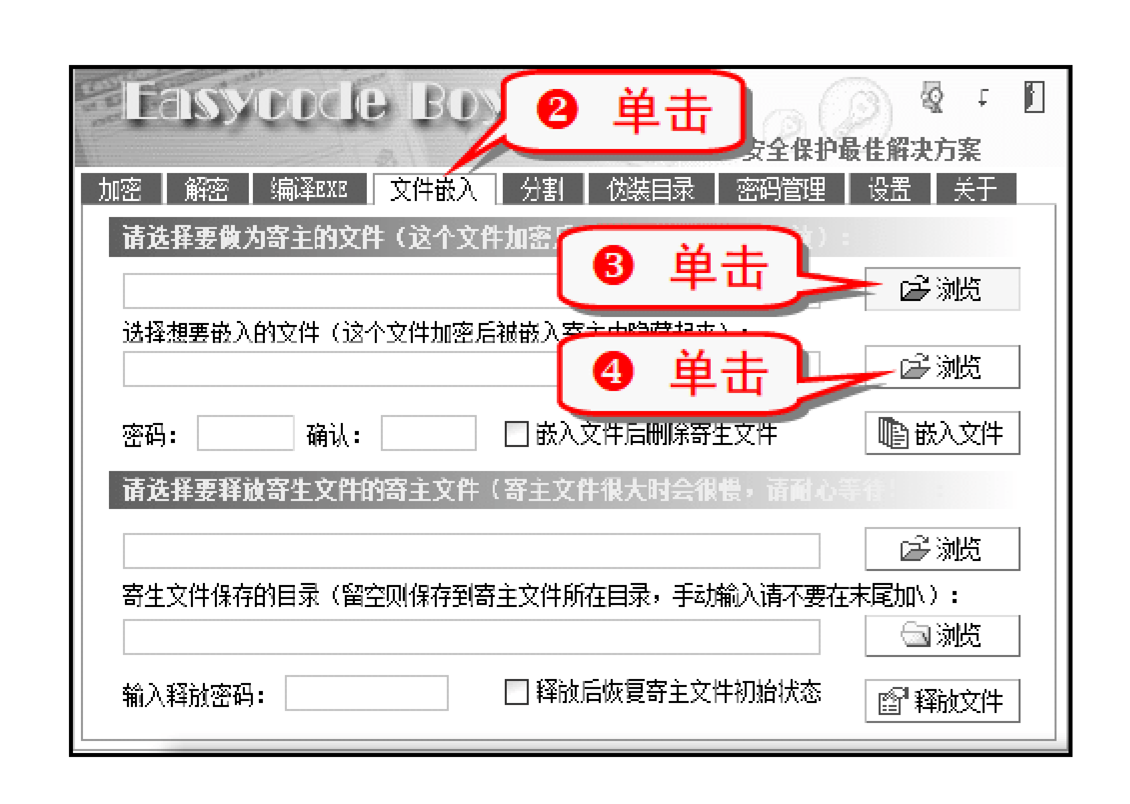


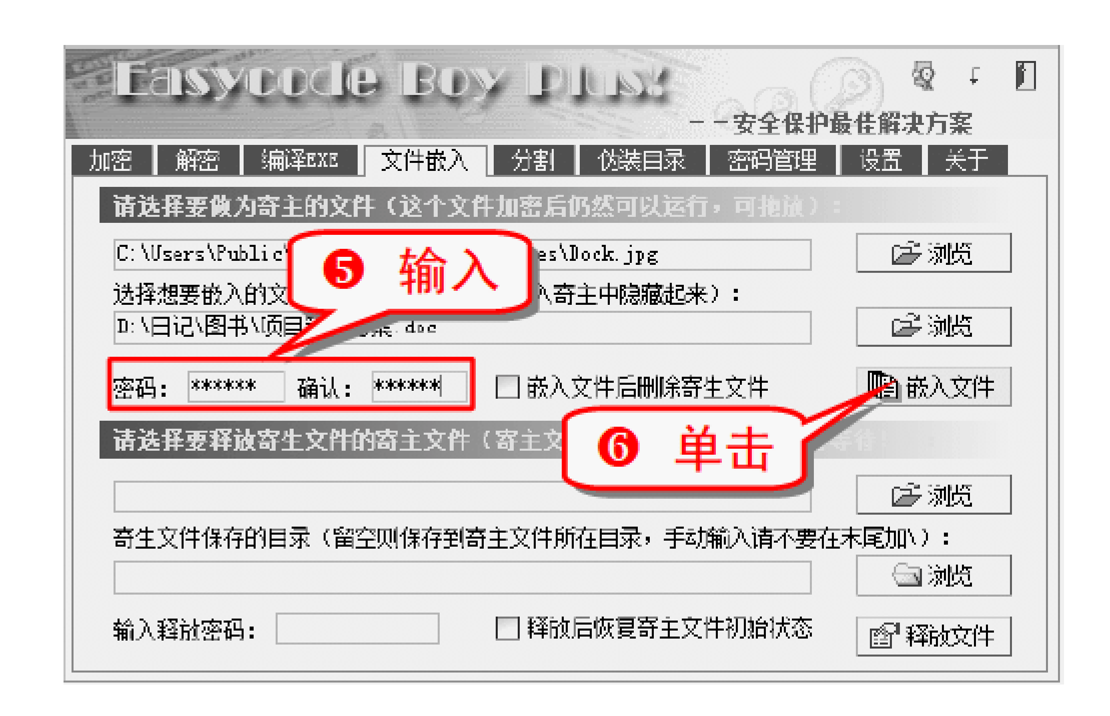
技巧39　在普通图片中隐藏文件

隐藏文件还有一种方法就是把文件藏在一张普通的图片中，它可以利用万能加密器实现。

万能加密器具有加密文件大小不限、文件类型不限以及加密速度快等特点，在很多网站都可以下载到它的最新版。下载并安装完成后，双击其运行程序即可使用。

❶ 运行万能加密器，弹出如下图所示的窗口。





举　一　反　三

利用万能加密器还能进行文件的加密、解密、分割以及伪装目录等，其功能非常强大。

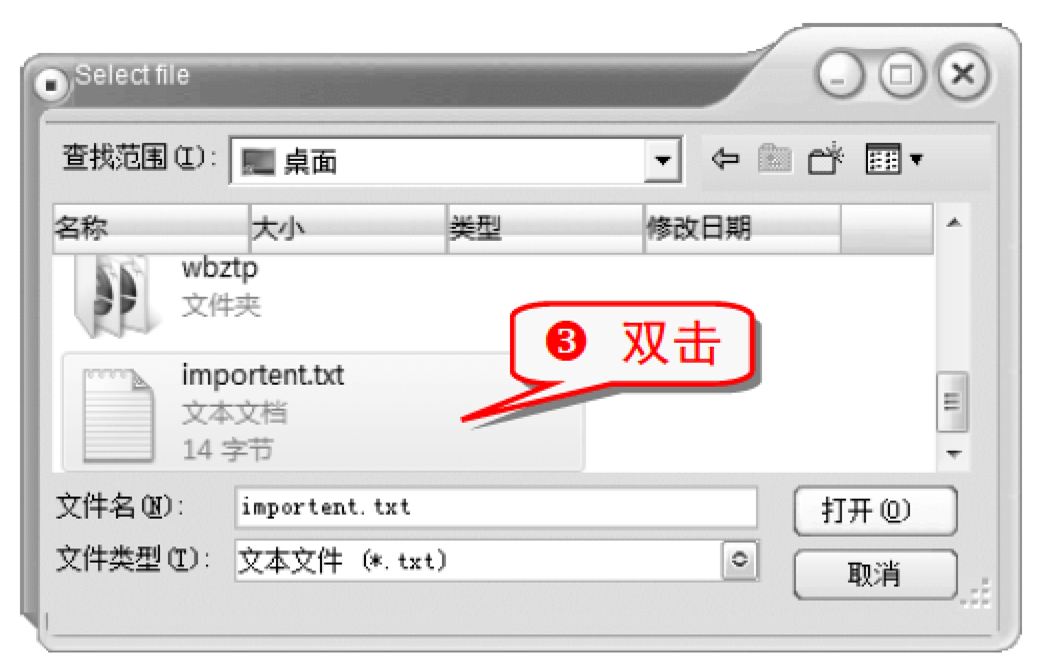
技巧40　用 txt2bmp 将记事本伪装成图片

记事本的安全性很低，为了防止别人随意查看记事本文件的内容，可以用 txt2bmp 将记事本文件伪装成图片文件。

(1) 将记事本文件隐藏到 BMP 文件中

❶ 安装并运行 txt2bmp 软件，弹出如下图所示的窗口。









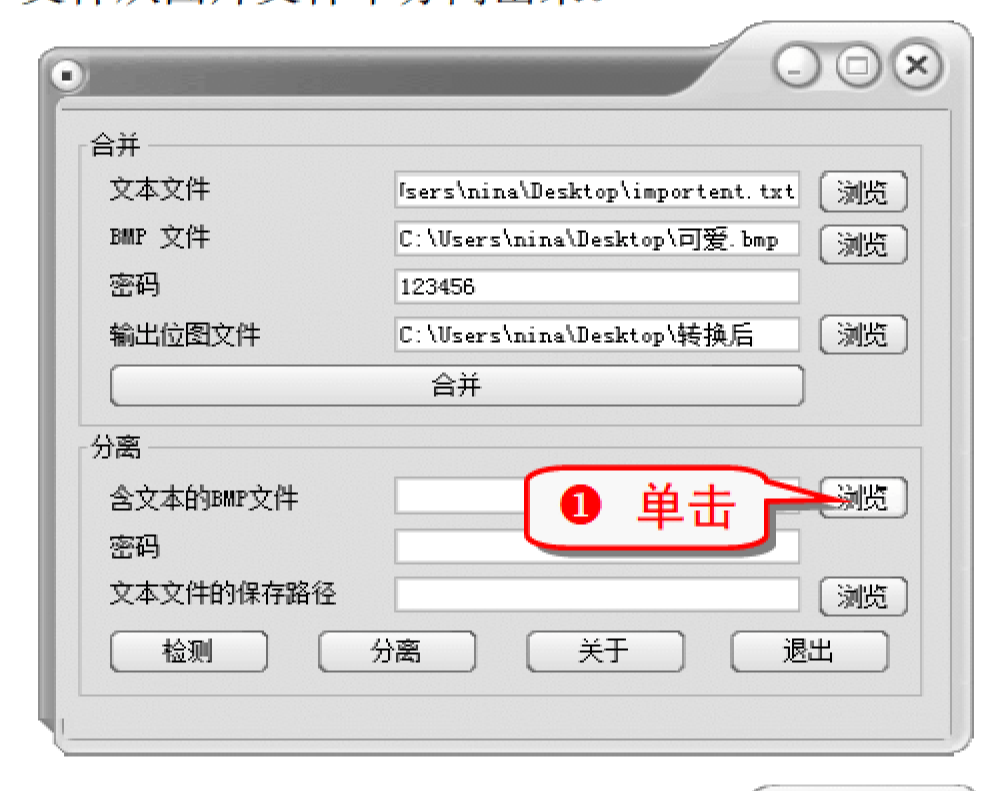






(2) 将文本文件分离出来

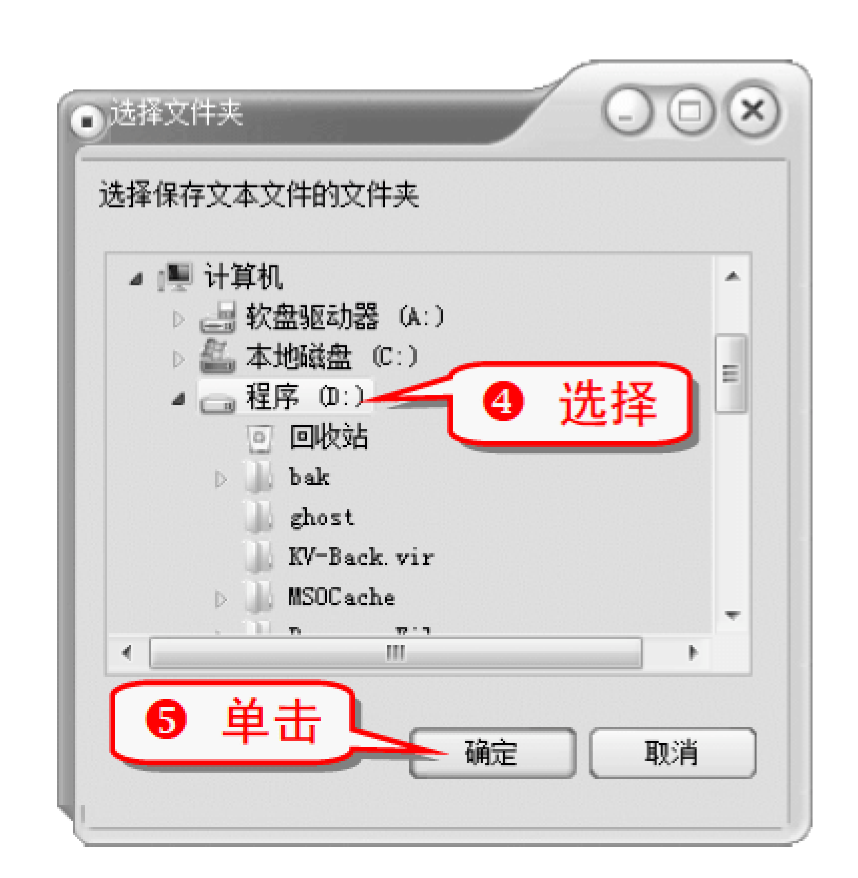
使用 txt2bmp，可以在用户需要查看文本文件时，将文本文件从图片文件中分离出来。









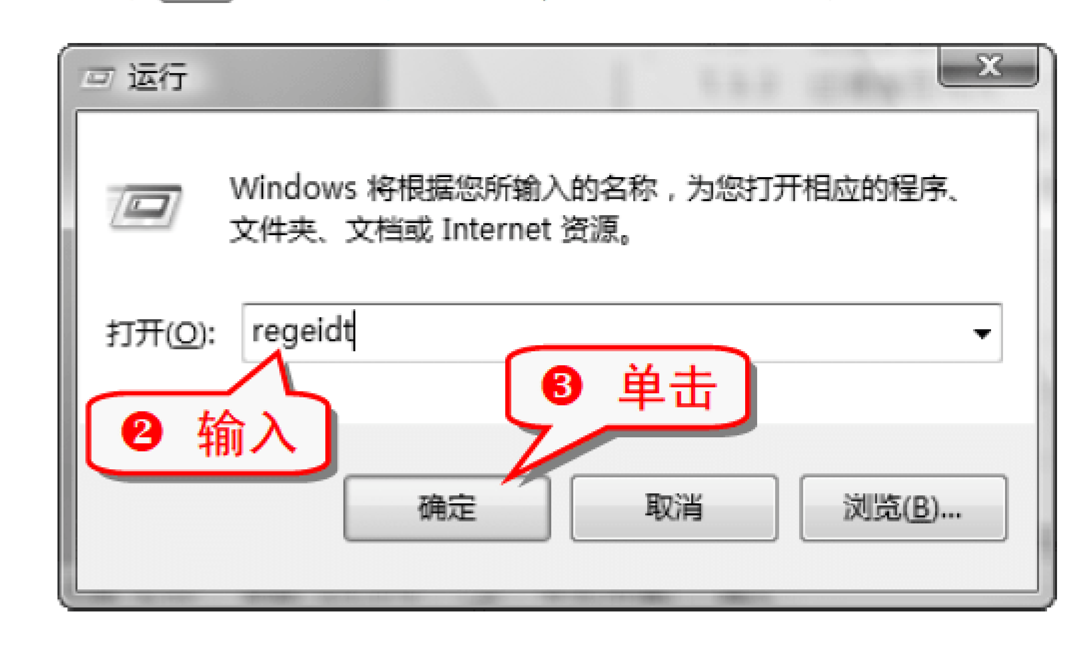




技巧41　隐藏驱动器

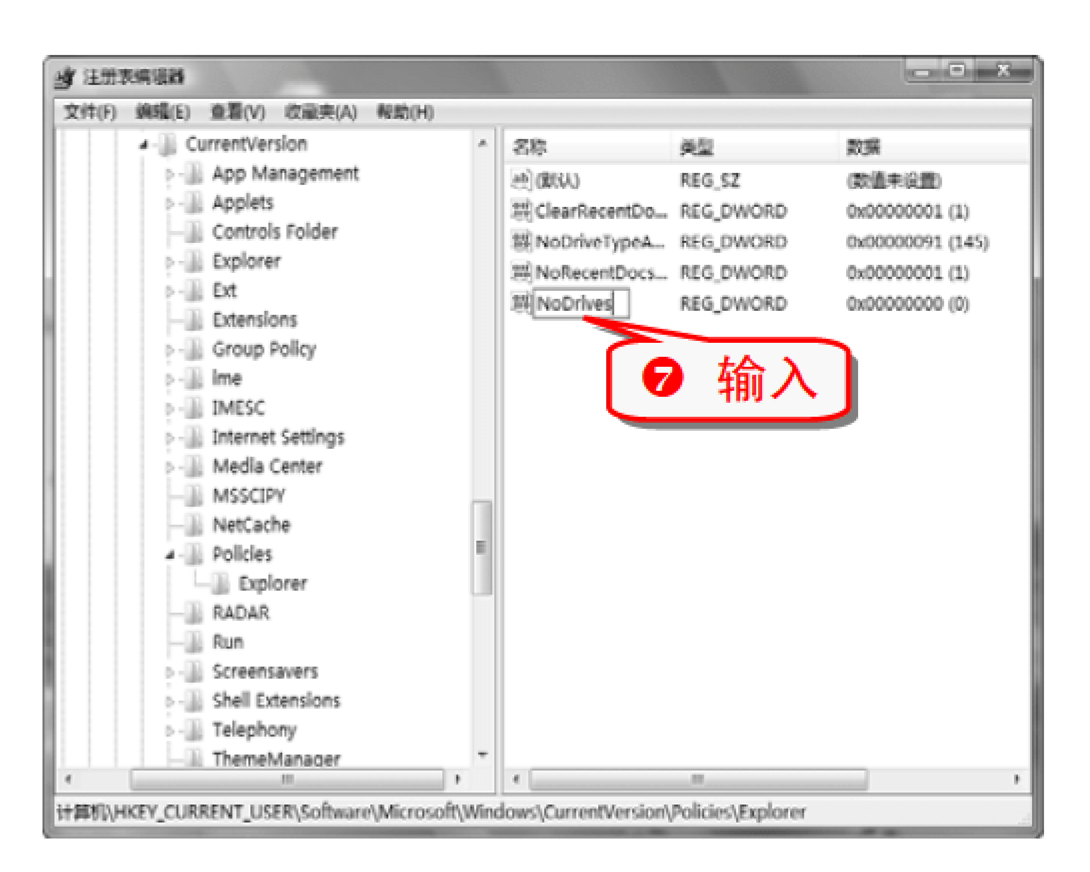
隐藏驱动器是文件与文件夹加密的有效手段，可以通过修改注册表的方式来实现驱动器的隐藏。

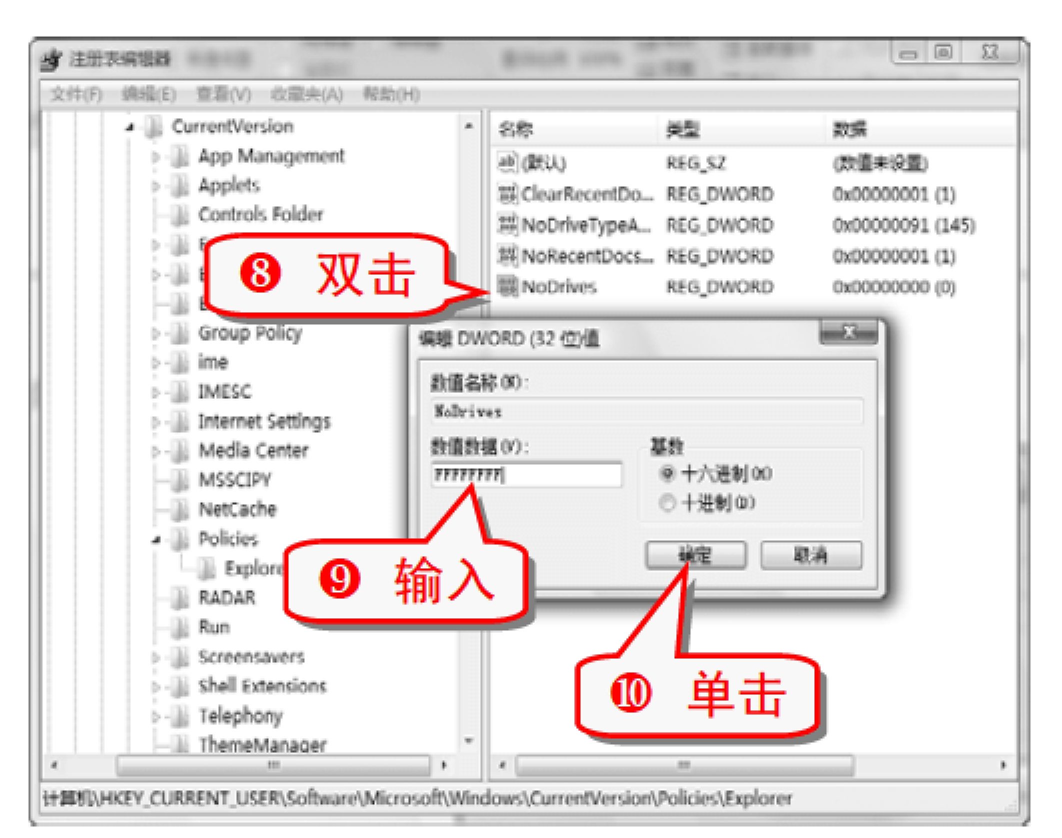
❶ 按下 ⊞ + R 组合键，弹出“运行”对话框。



❹ 在弹出的注册表编辑器中展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支。







举　一　反　三

将 NoDrives 的值改为 4，就可以隐藏 C 盘；将 NoDrives 的值改为 8，就可以隐藏 D 盘；将 NoDrives 的值改为 10，就可以隐藏 E 盘。

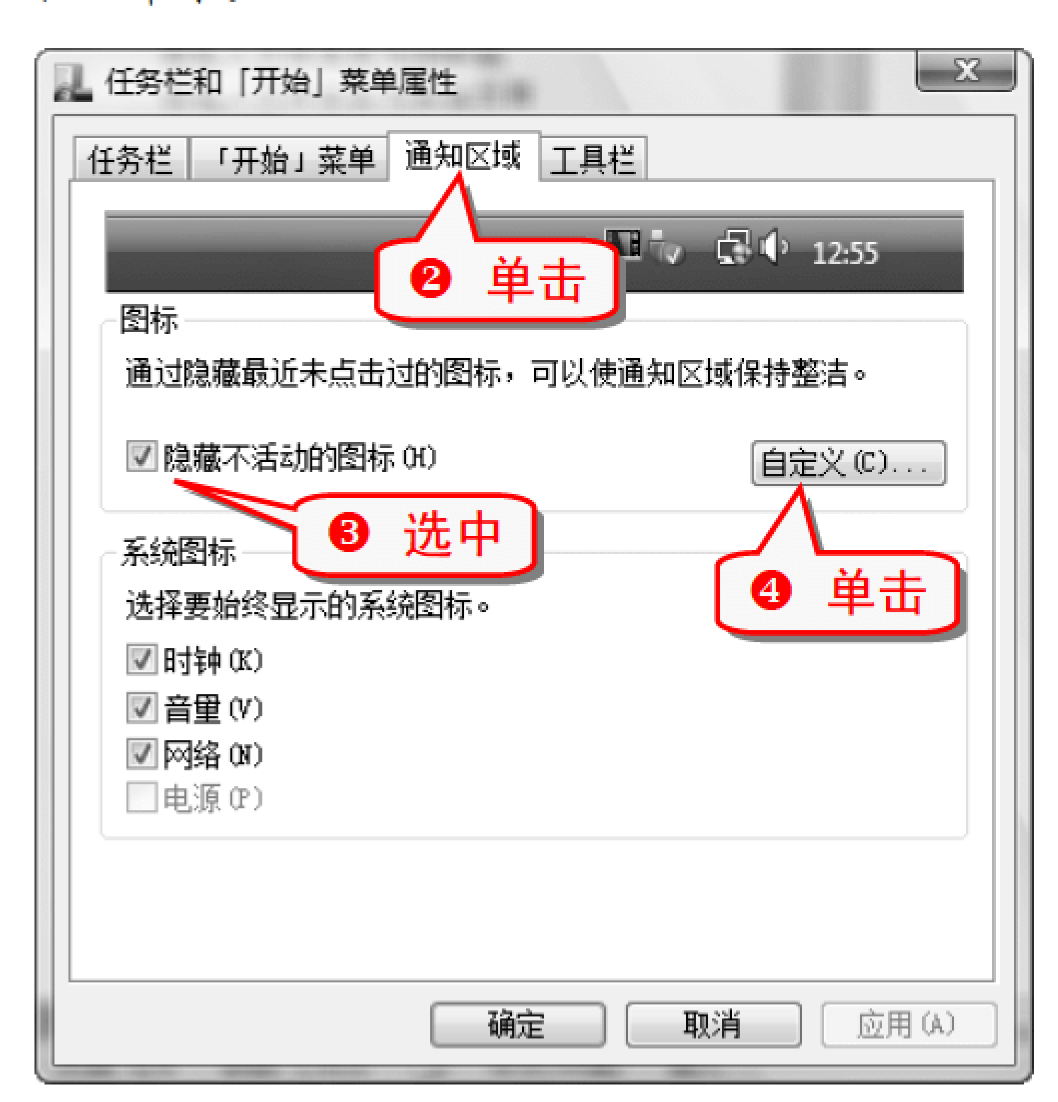
知　识　补　充

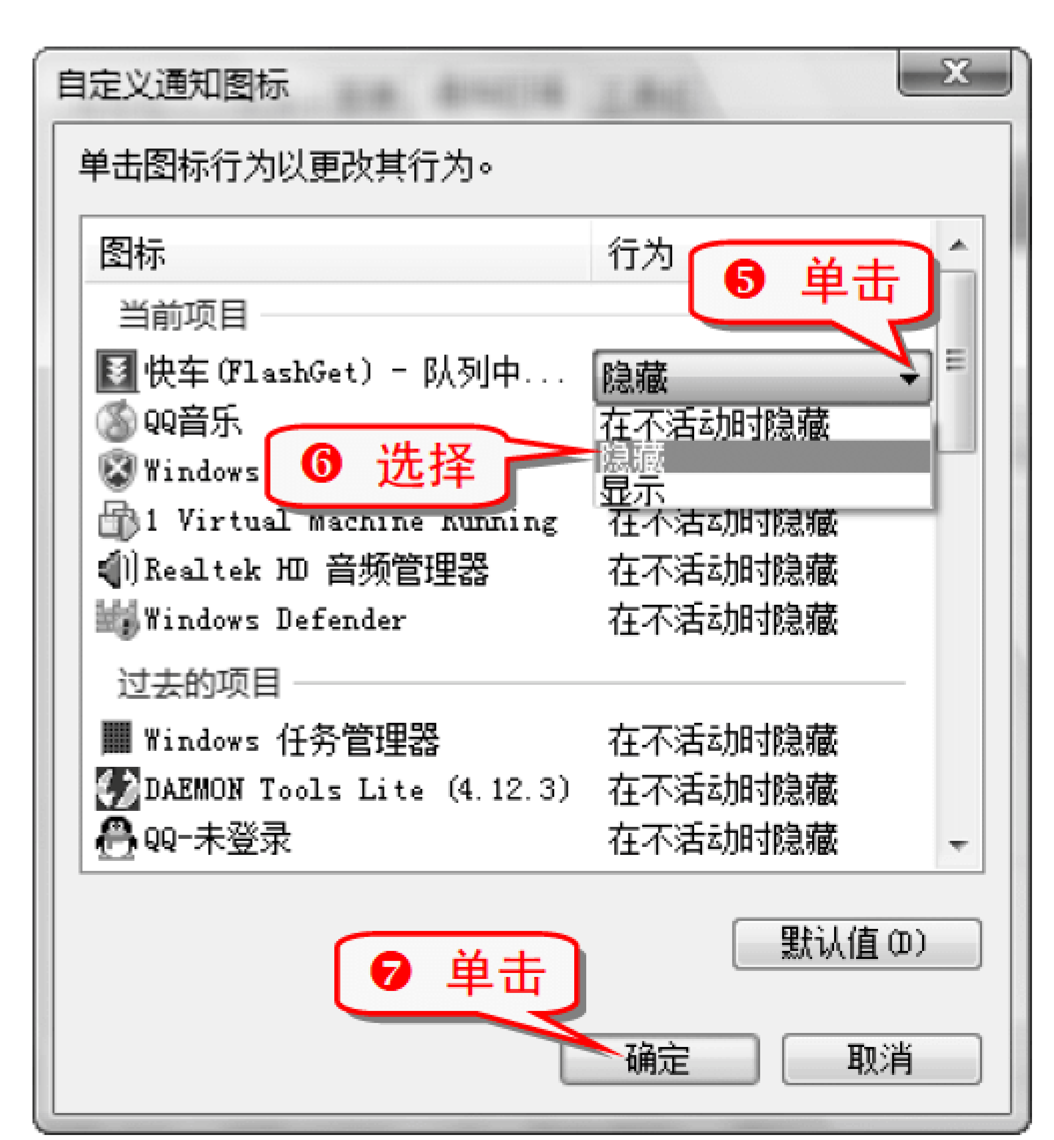
将 NoDrives 的值改为 0 或将其删除可以使被隐藏的驱动器重新显示出来。

技巧42 隐藏通知区域的程序图标

当前系统正在运行什么程序都可以从通知区域看到，如果不想让这些图标被看到，可以将其隐藏起来。

❶ 右击任务栏的空白地方，在弹出的快捷菜单中选择“属性”命令。







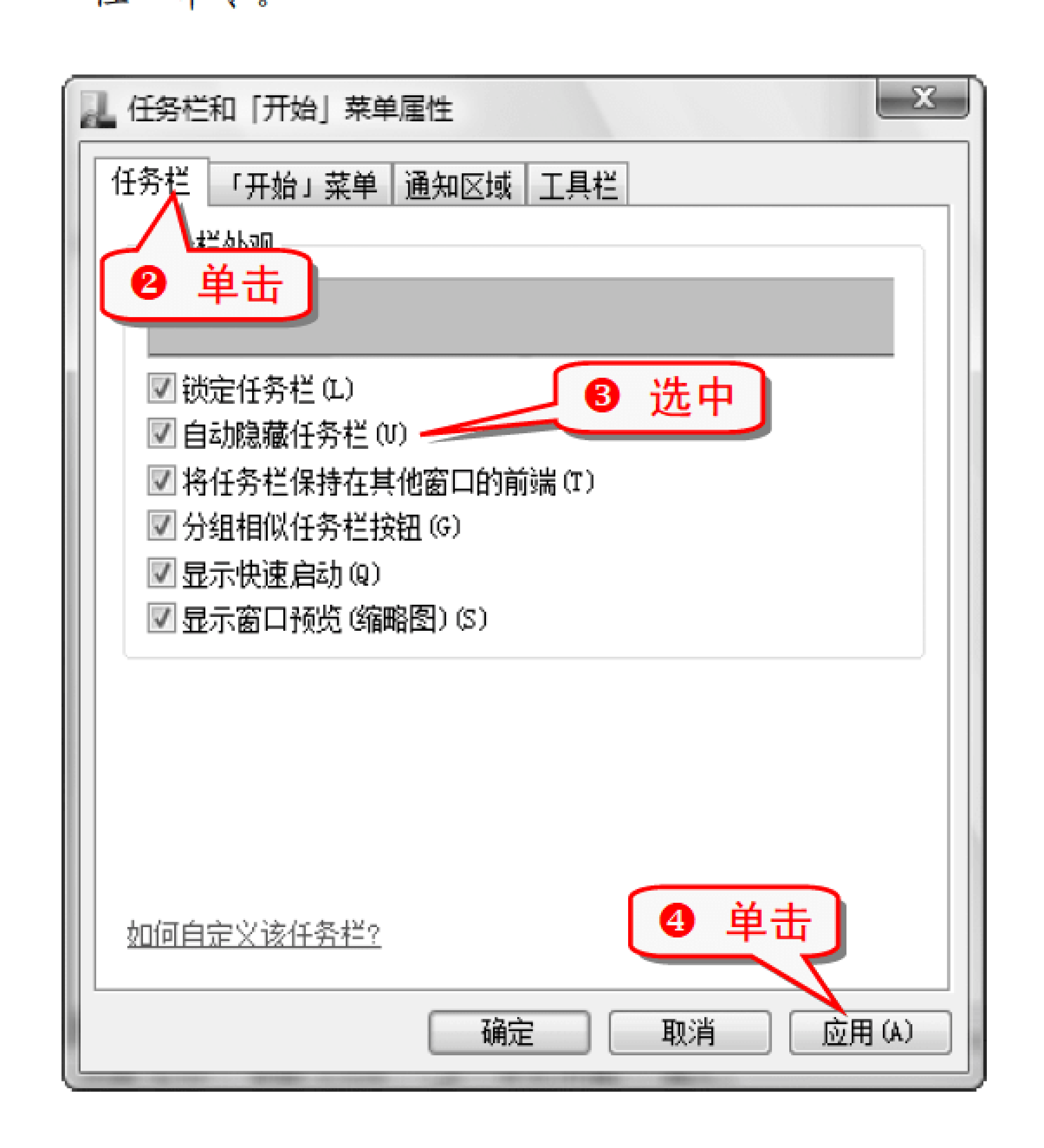
知 识 补 充

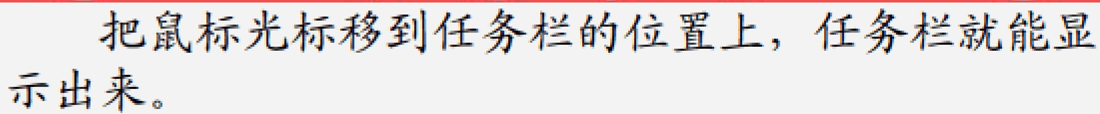
在通知区域可以看到：16:51，FlashGet 的图标不见了。只有单击◀，才可以看到其图标。

技巧43 自动隐藏任务栏

隐藏通知区域的图标，并不能隐藏所有在运行的程序，通过设置可以将整个任务栏隐藏起来。

❶ 右击任务栏的空白地方，在弹出的快捷菜单中选择“属性”命令。



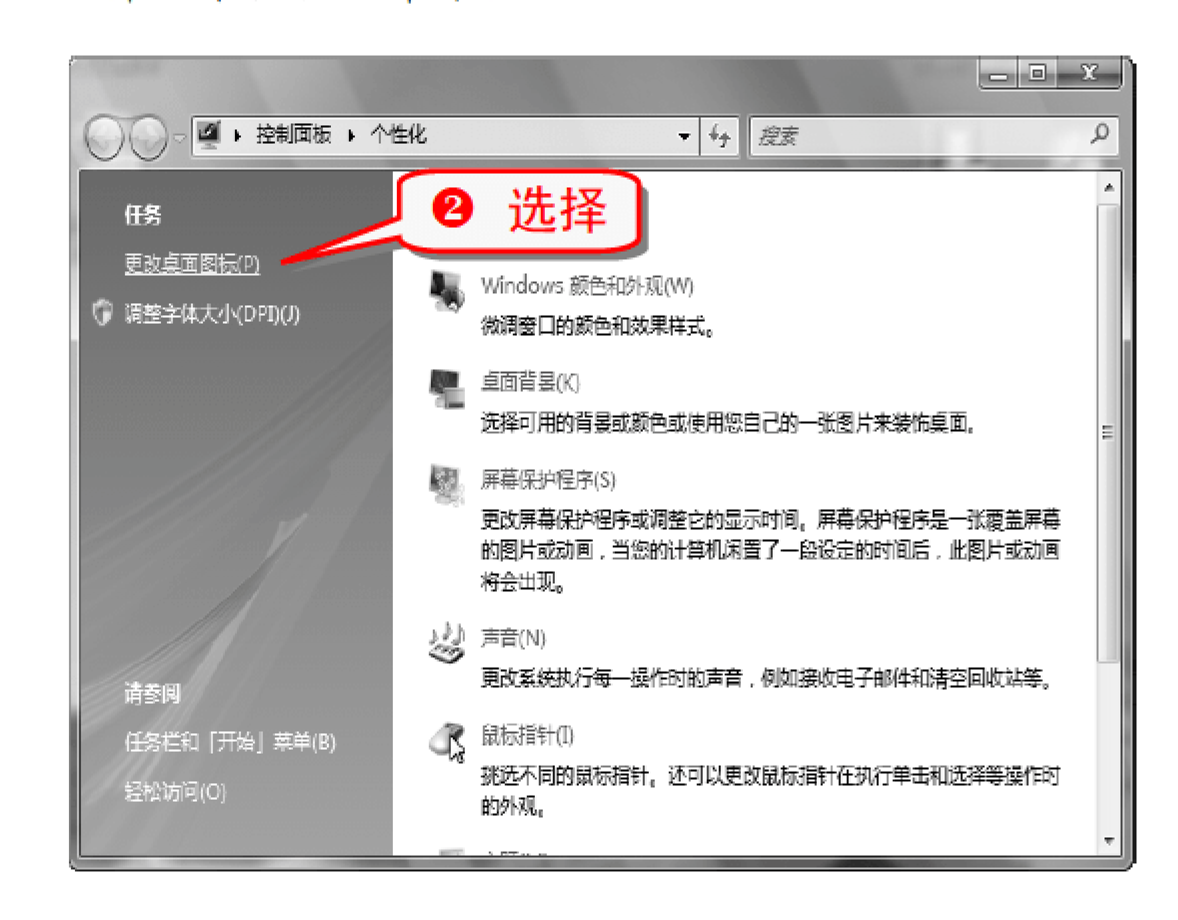


把鼠标光标移到任务栏的位置上，任务栏就能显示出来。

技巧44 使回收站从桌面上消失

回收站是黑客比较喜欢逛的地方，里面会有很多被删除的隐私文件，如果没有彻底删除文件的习惯，不妨将回收站隐藏起来。

❶ 右击计算机桌面的空白地方，在弹出的快捷菜单中选择“个性化”命令。







专　家　坐　堂

把回收站隐藏以后，在桌面上建一个没有用的文件夹，将其伪装成回收站，这样的效果会更好。

技巧45　快速隐藏桌面程序图标

通过简单的设置可以让桌面上所有的图标都不可见。

❶ 右击桌面的空白处。





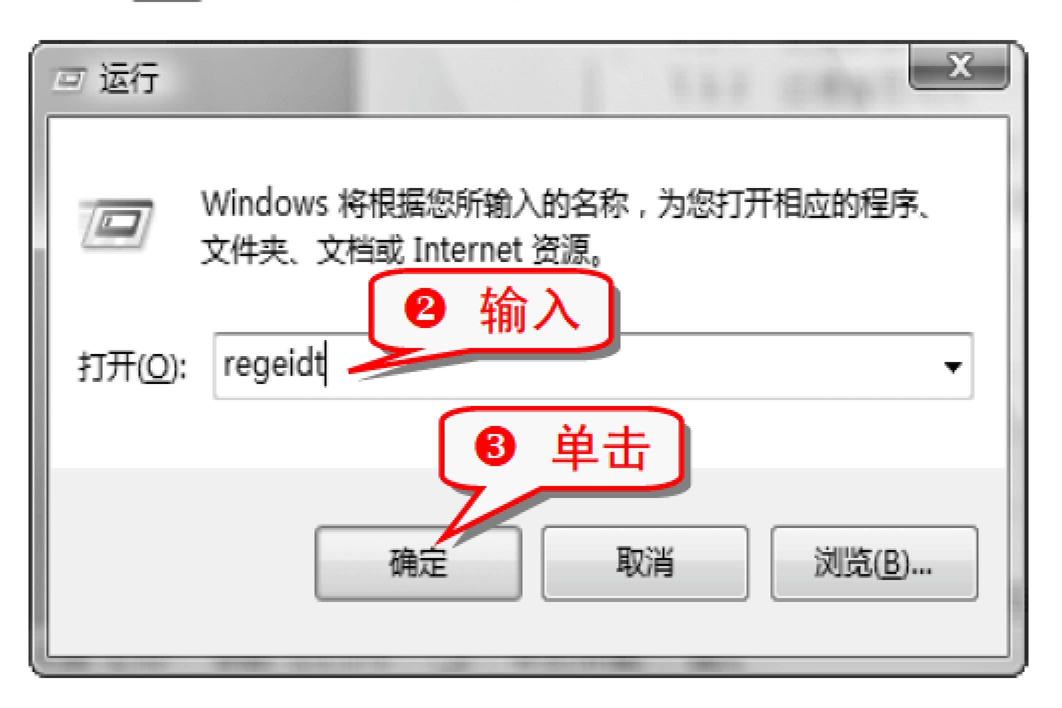
知　识　补　充

想要让程序图标重新显示在桌面上，只需要右击桌面空白处，在弹出的快捷菜单中选择“查看”→“显示桌面图标”就可以了。

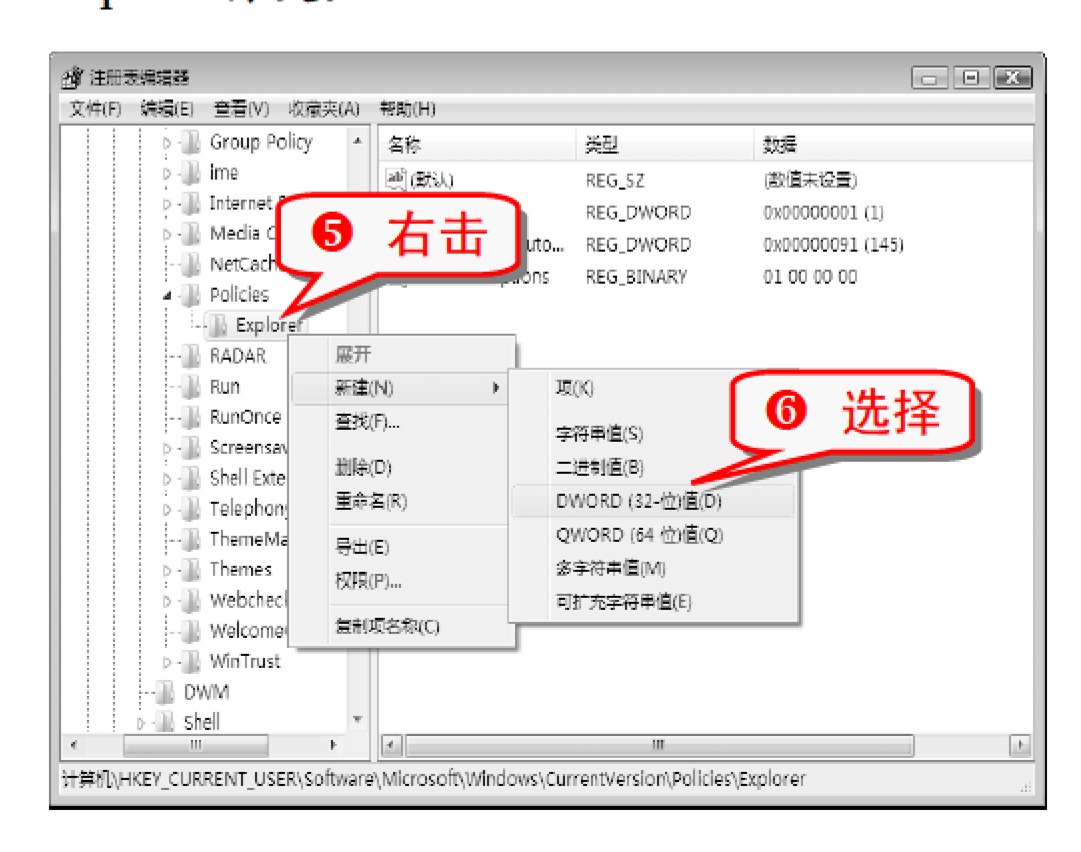
技巧46　彻底隐藏“网络”图标

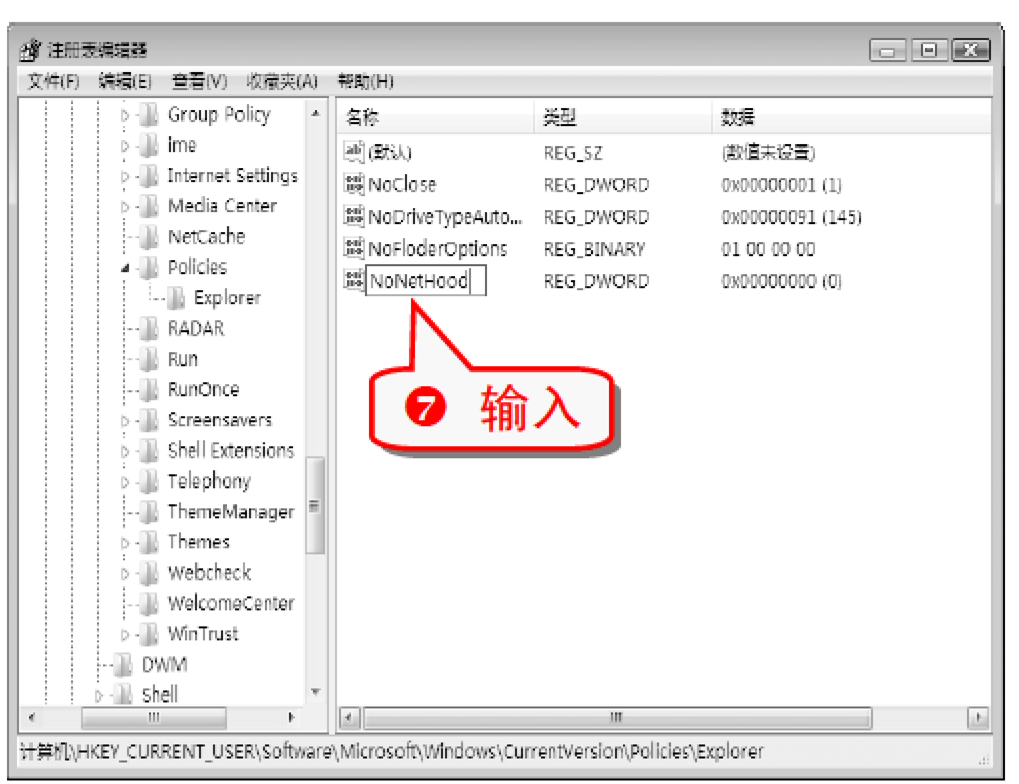
如果隐藏“网络”图标，则黑客就无法直接通过当前电脑入侵局域网内的其他电脑。

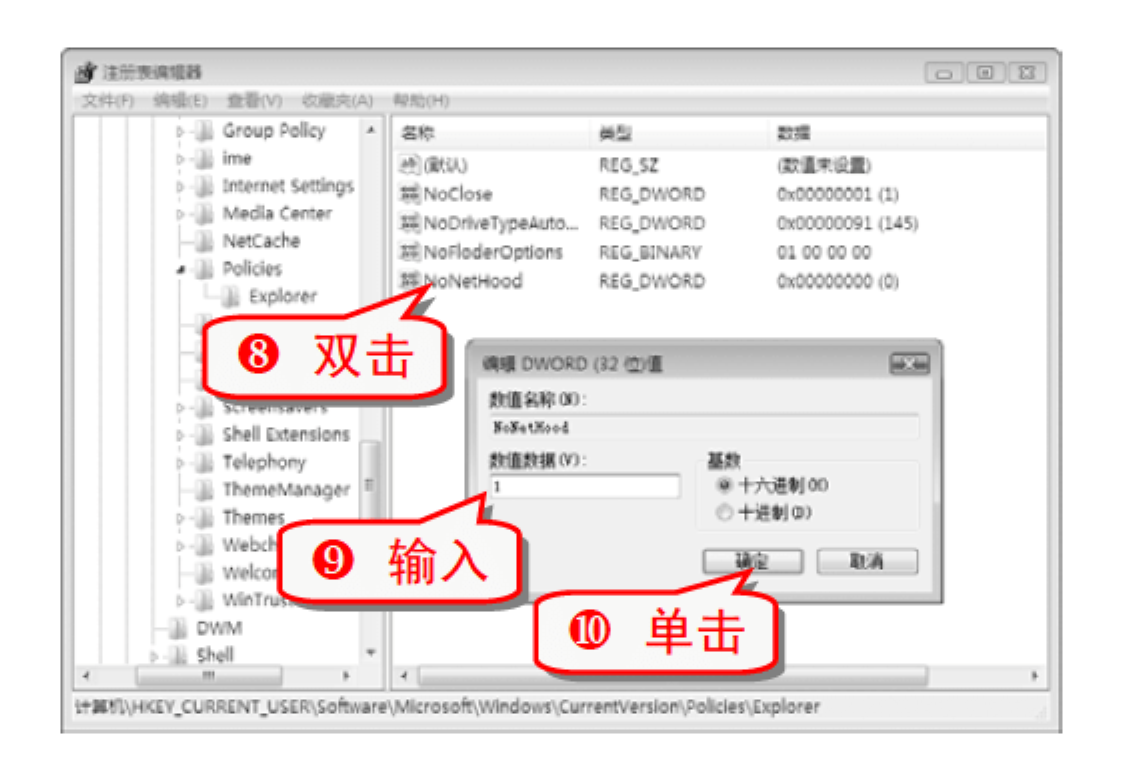
❶ 按下 ⊞ + R 组合键，弹出“运行”对话框。



❹ 在弹出的注册表编辑器中展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支。







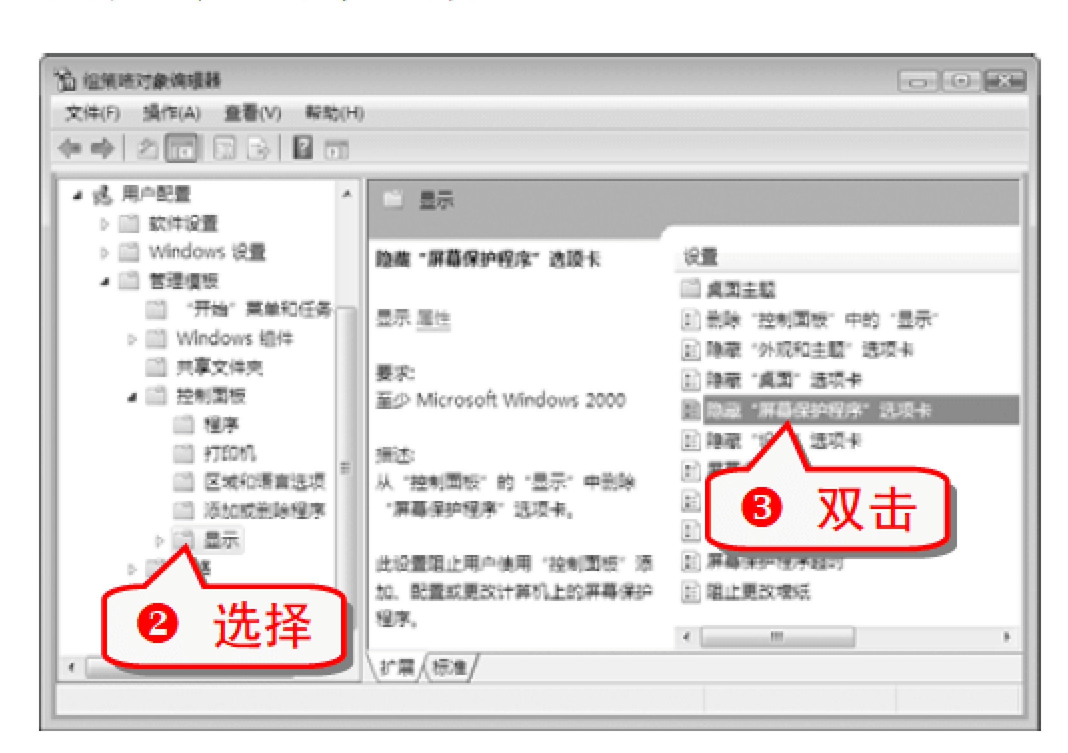
知 识 补 充

想要让"网络"图标重新显示在桌面上，只需要将上述步骤中新建的键值删除即可。

技巧47 隐藏"屏幕保护程序"选项卡

隐藏"屏幕保护程序"选项卡可以阻止黑客添加、配置或更改电脑上的屏幕保护程序。

❶ 打开组策略对象编辑器。





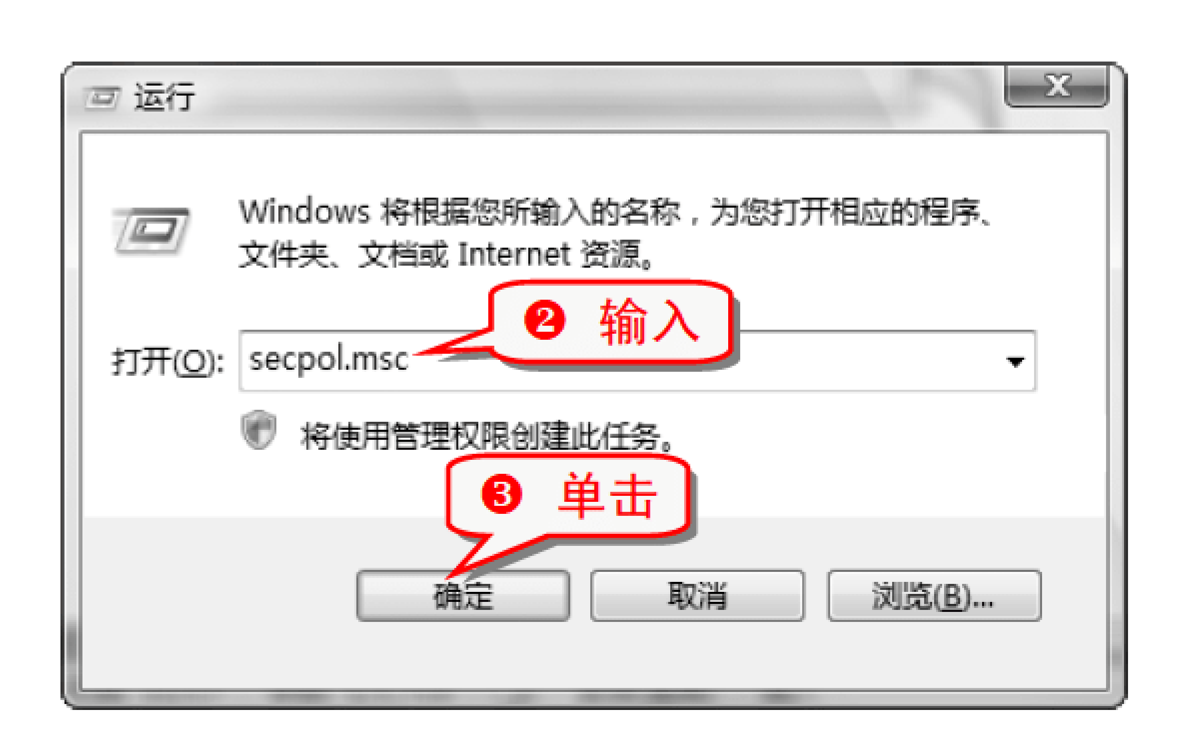
❻ 右击桌面空白处，在弹出的快捷菜单中选择"个性化"命令，在弹出的"个性化"窗口中可以看到没有"屏幕保护程序"了。

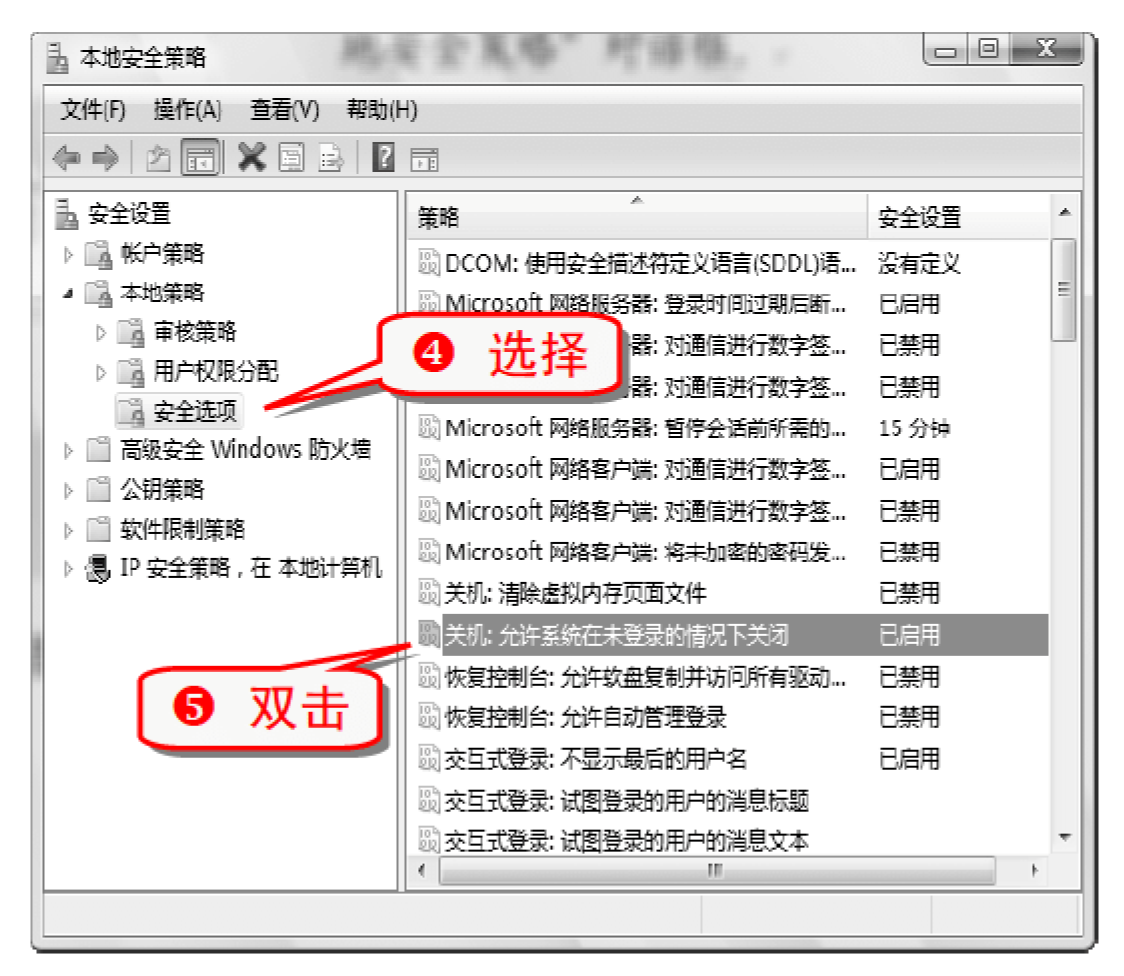


技巧48 使关机按钮从登录界面消失

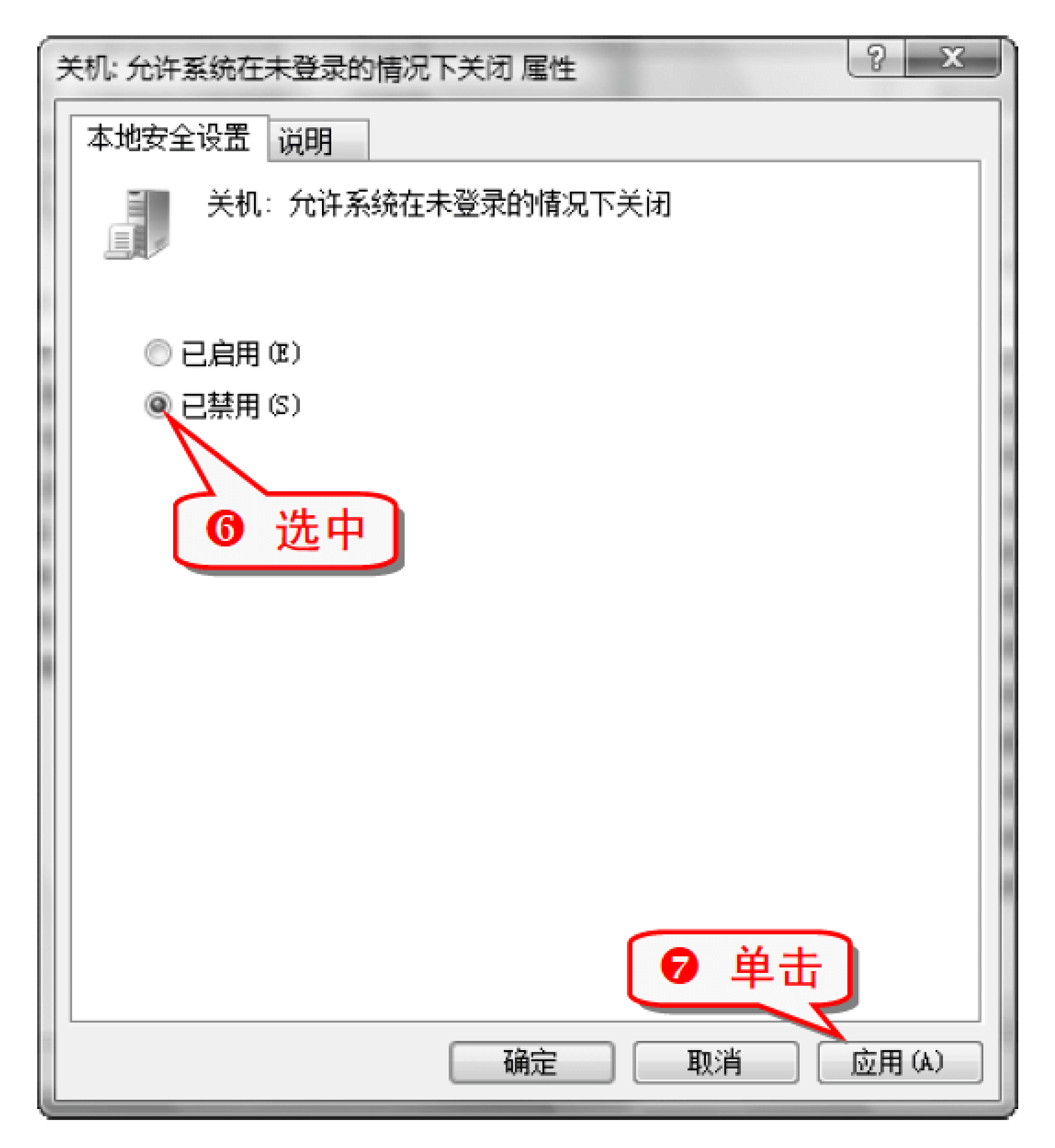
登录界面上的关机按钮可以让电脑非法关机，破除电脑的屏幕保护状态，如果觉得关机按钮没有什么用，还是将其隐藏比较好。

❶ 按下 ⊞ + R 组合键，弹出"运行"对话框。









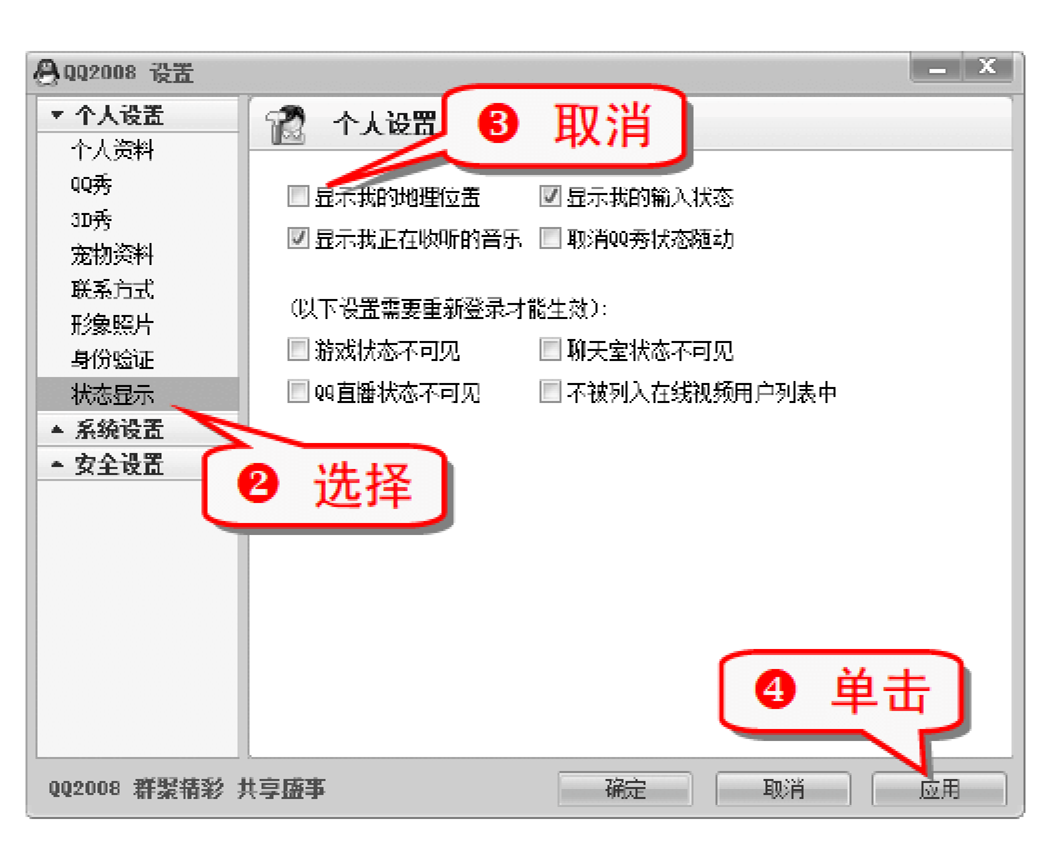




技巧49　隐藏 QQ 2008 的地理位置

使用 QQ 2008 的时候，可以通过查看 QQ 好友的地理位置知道好友在哪个城市，如果不想暴露自己的地理位置，可以通过以下几个步骤进行隐藏设置。

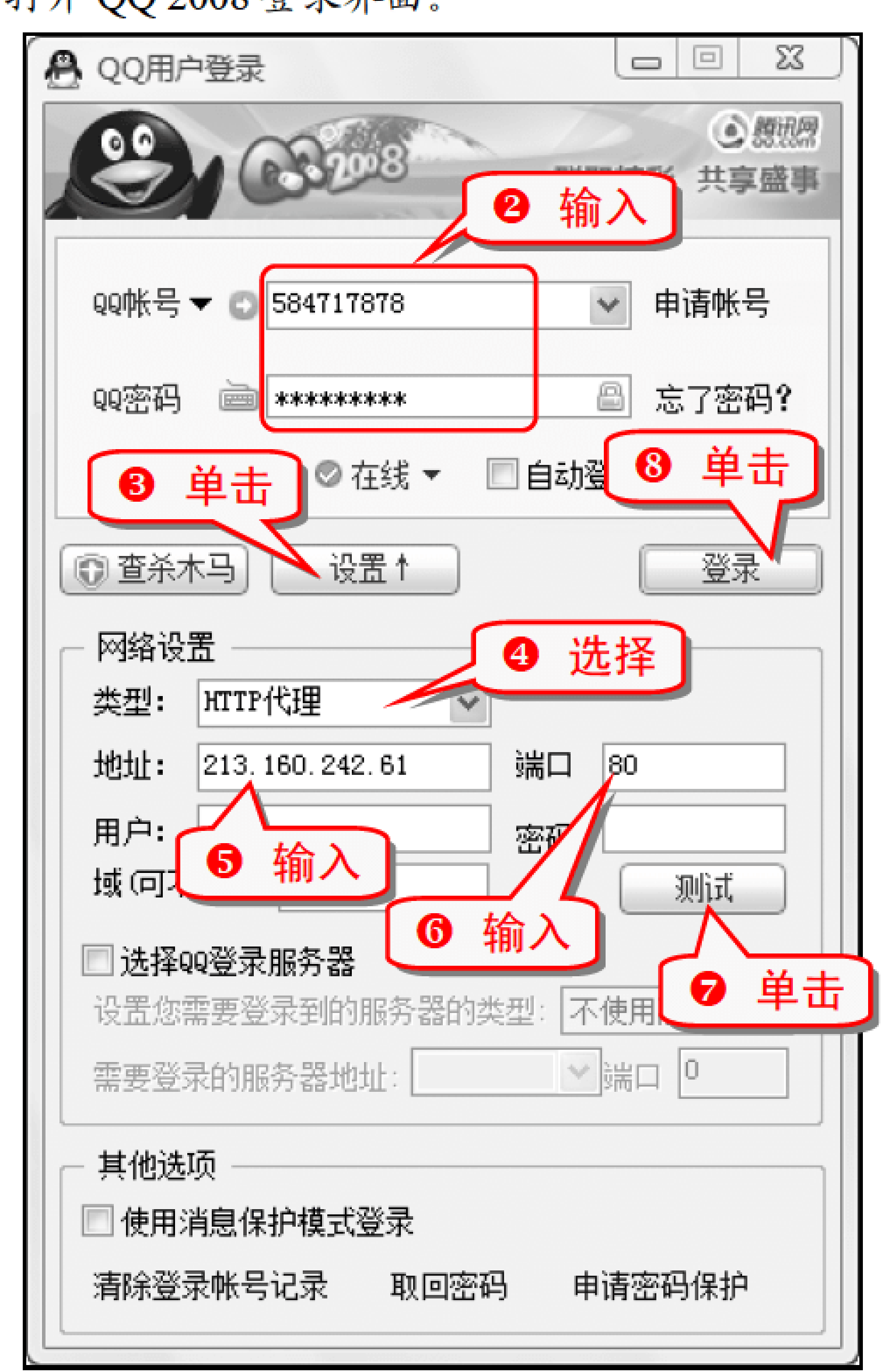
❶ 登录 QQ 2008，选择“系统菜单”→“设置”→“个人设置”命令，弹出“QQ 2008 设置”窗口。



技巧50　用代理服务器伪装 QQ 2008 的 IP

通过代理服务器登录上 QQ，这样攻击者所看到的 IP 地址是代理服务器的 IP 地址。

❶ 打开 QQ 2008 登录界面。



注 意 事 项

上述设置过程中如果测试代理失败则换一个代理 IP 和端口，这些都可以在网上找到。

这里介绍几个免费的代理网站，上面可以找到很多的代理 IP。如 http://web.proxycn.com/ 和 http://fast.proxycn.com/proxy30/page1.htm。





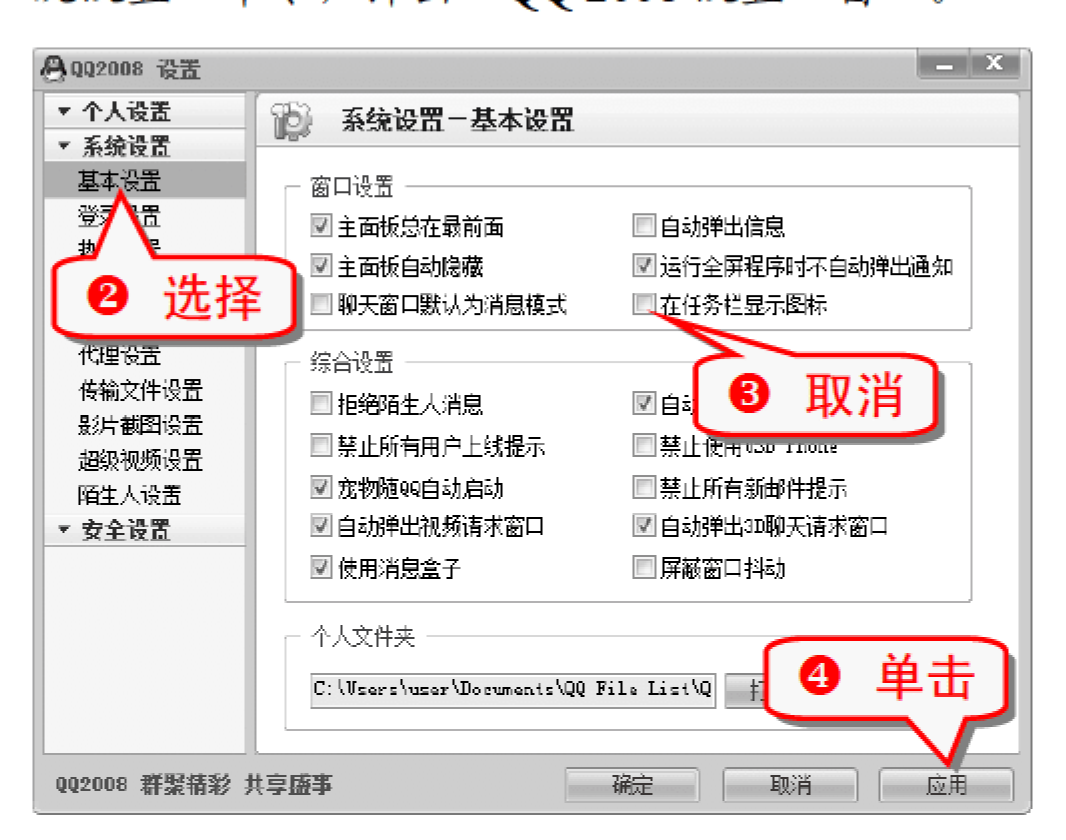
举 一 反 三

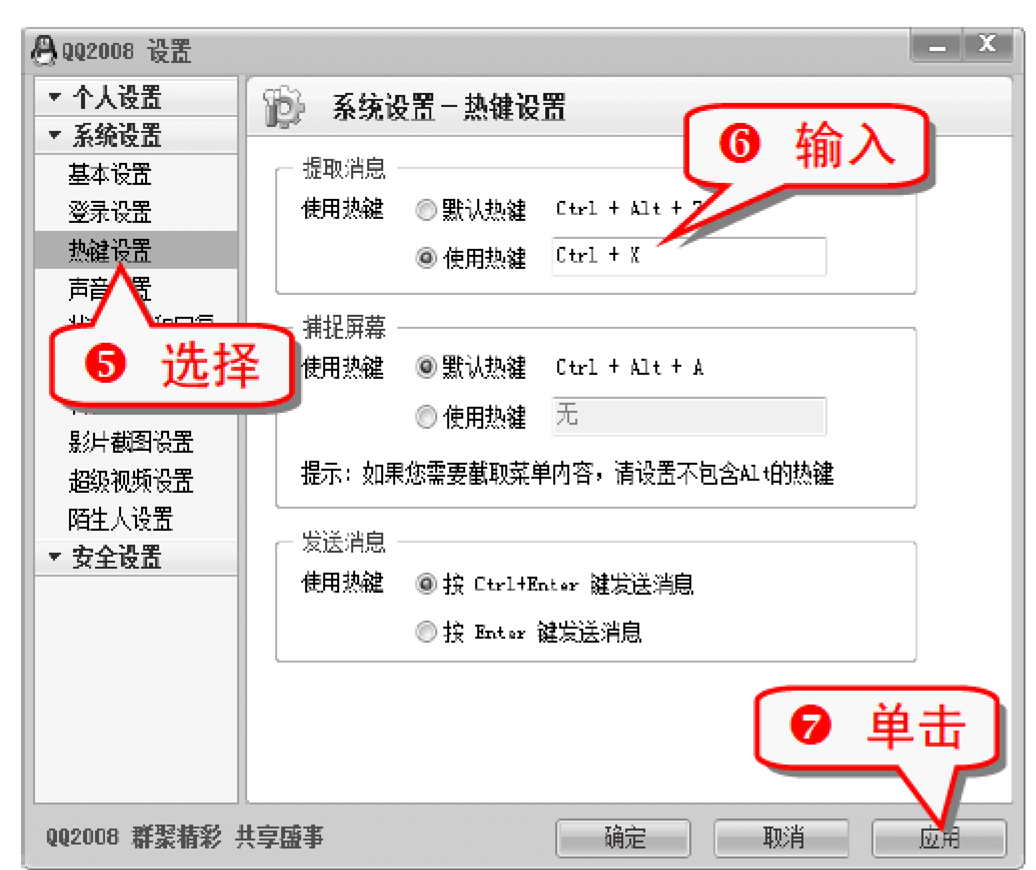
隐身登录的消息传递是通过服务器中转的，这样传给攻击者的数据包的 IP 地址是腾讯服务器的地址，同样也起到了隐藏 IP 的效果。

技巧51 使别人不知道自己已登录

平常上网的时候，会经常要去干些别的事情，就将 QQ 挂在那里，然后离开电脑，这样是很不安全的。通过简单的几步设置，可以让人看不出电脑中有 QQ 登录者。

❶ 登录 QQ 2008，选择“系统菜单”→“设置”→“系统设置”命令，弹出“QQ 2008 设置”窗口。







注 意 事 项

上述步骤的热键选择要看个人习惯，不一定要选择 Ctrl + X 组合键。

通过上述步骤的设置，可以发现把 QQ 最小化以后只有按下 Ctrl + X 组合键才能把 QQ 界面调出来。



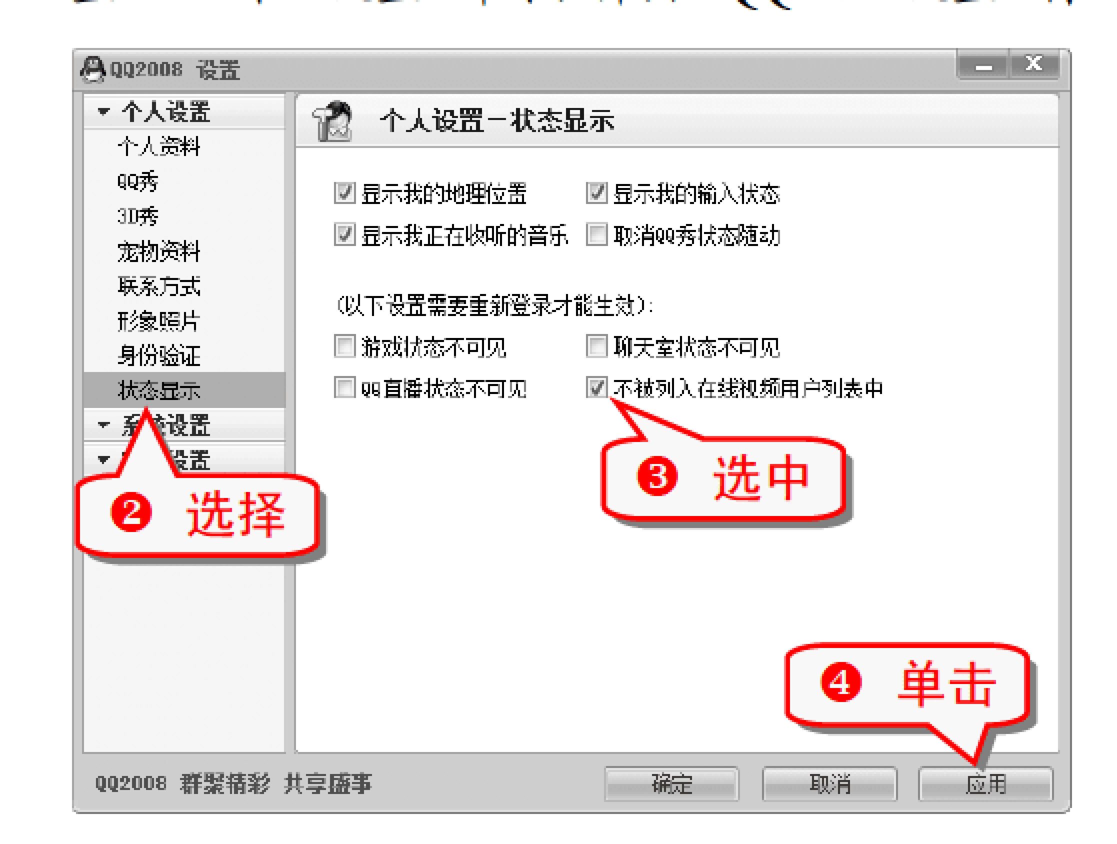
专 家 坐 堂

通过任务管理器可以查看到有没有 QQ 在运行，所以在选择“提取消息”的热键时，尽量不要选用默认的热键。

技巧52 巧妙隐藏 QQ 2008 的摄像头

摄像头可以给 QQ 聊天带来很大的方便，同时也带来了很多的麻烦，经常会被骚扰。其实只要将摄像头隐藏起来，就没有那么多的烦恼了。

❶ 登录 QQ 2008，选择 QQ 面板上的“系统菜单”→“设置”→“个人设置”命令，弹出“QQ 2008 设置”窗口。





举 一 反 三

这里再介绍几种禁用摄像头的方法。

方法一：选择 QQ 面板上的“系统菜单”→“工具”→“语音视频调节”命令，在弹出的“语音视频调节向导”对话框中选择“下一步”，在“请选择你的视频设备”一栏选择“禁用”。

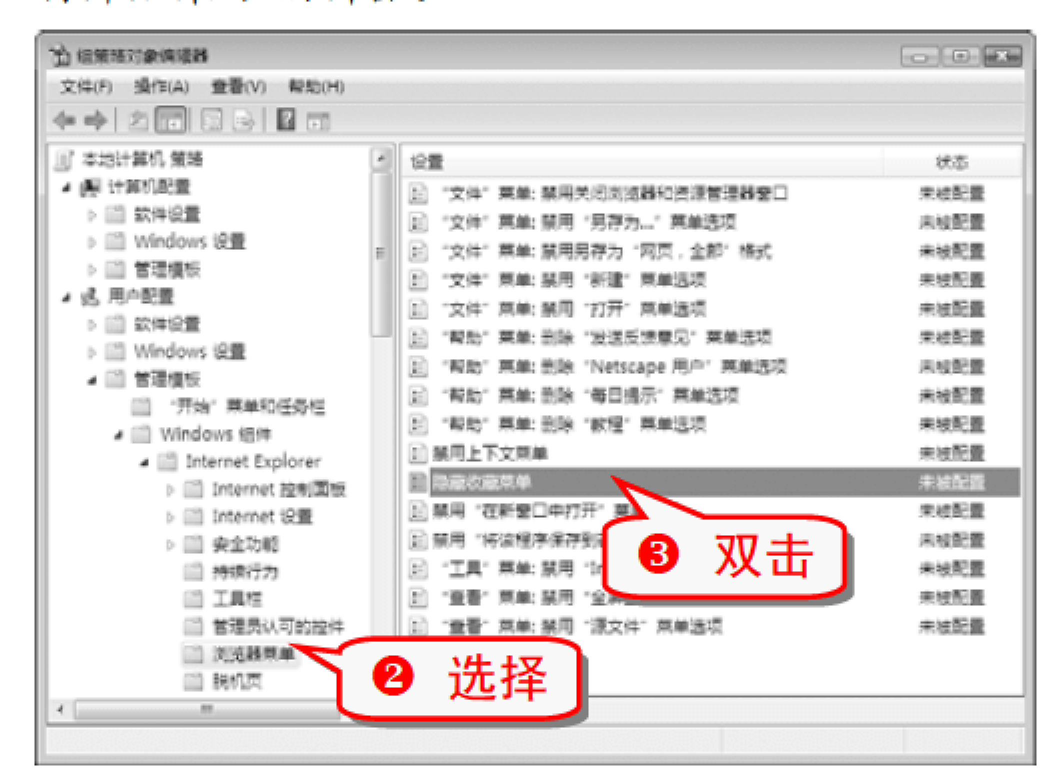
方法二：选择 QQ 面板上的“系统菜单”→“设置”→“系统设置”命令，在弹出的对话框中，将“禁止使用 USB Phone”选项选中，然后单击“应用”按钮。

方法三：直接把摄像头拔掉，但是这样比较麻烦，不建议使用这种方法。

技巧53 巧妙隐藏 IE 收藏夹

收藏夹中收藏着用户喜欢和常用的网址，给用户带来方便的同时也带来了安全隐患。通过组策略编辑器可以将收藏夹隐藏。

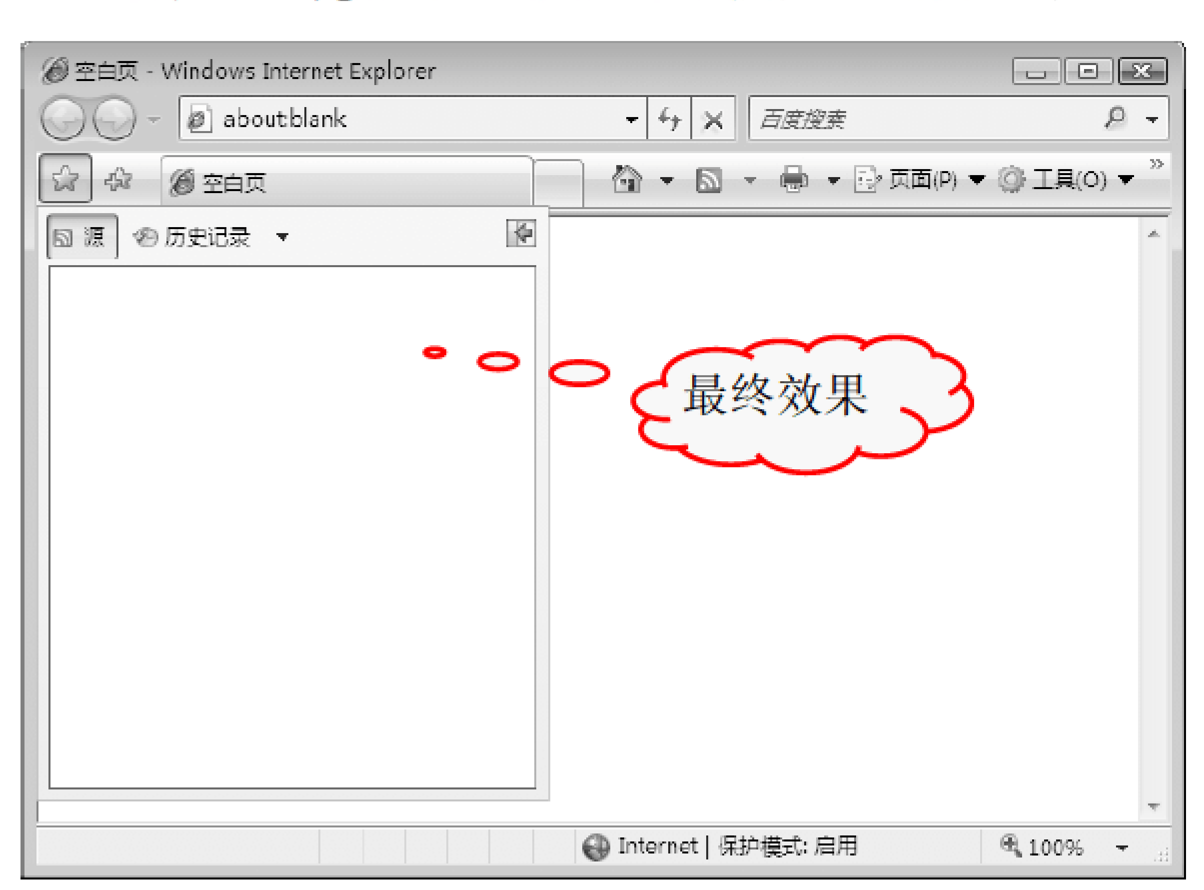
❶ 打开组策略编辑器。







❻ 打开 IE 浏览器可以发现，收藏夹里面是空白的。



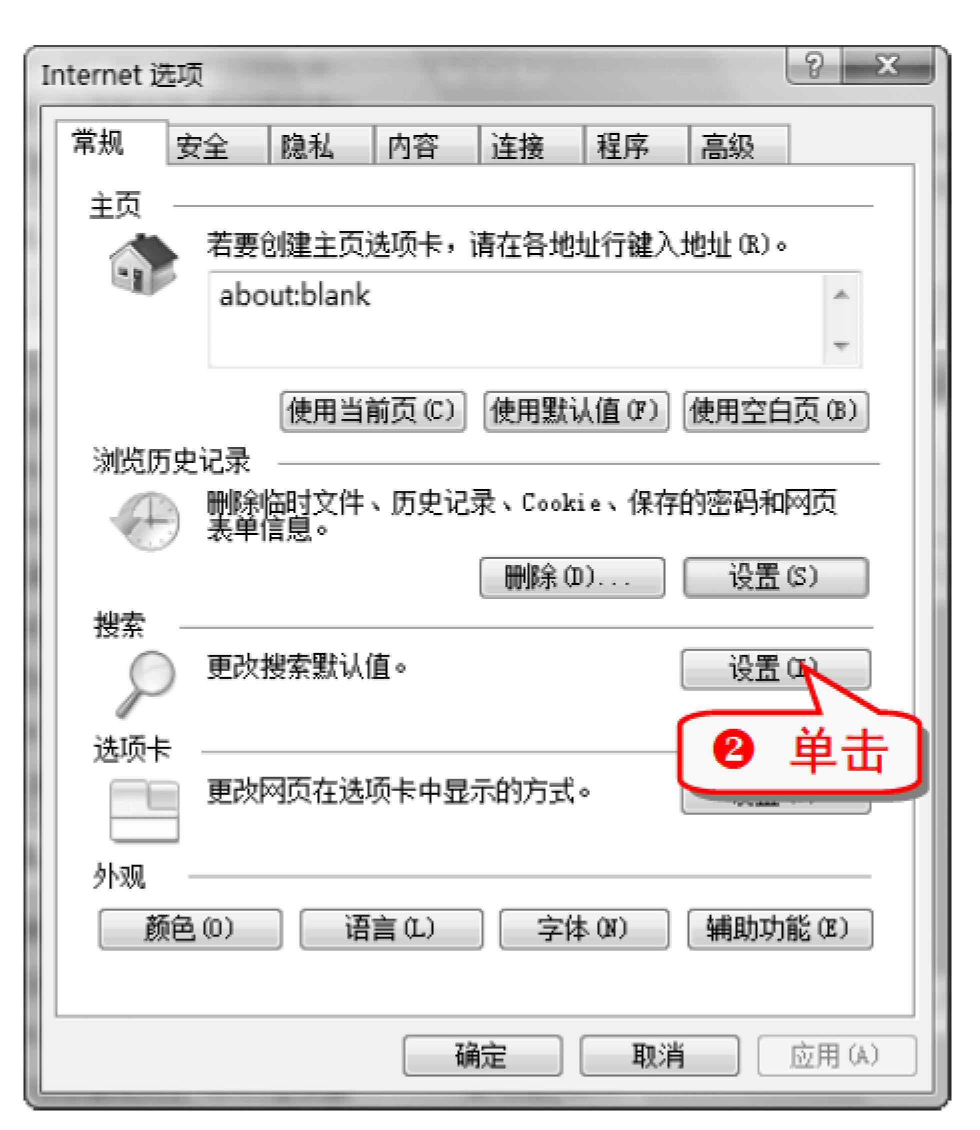
注　意　事　项

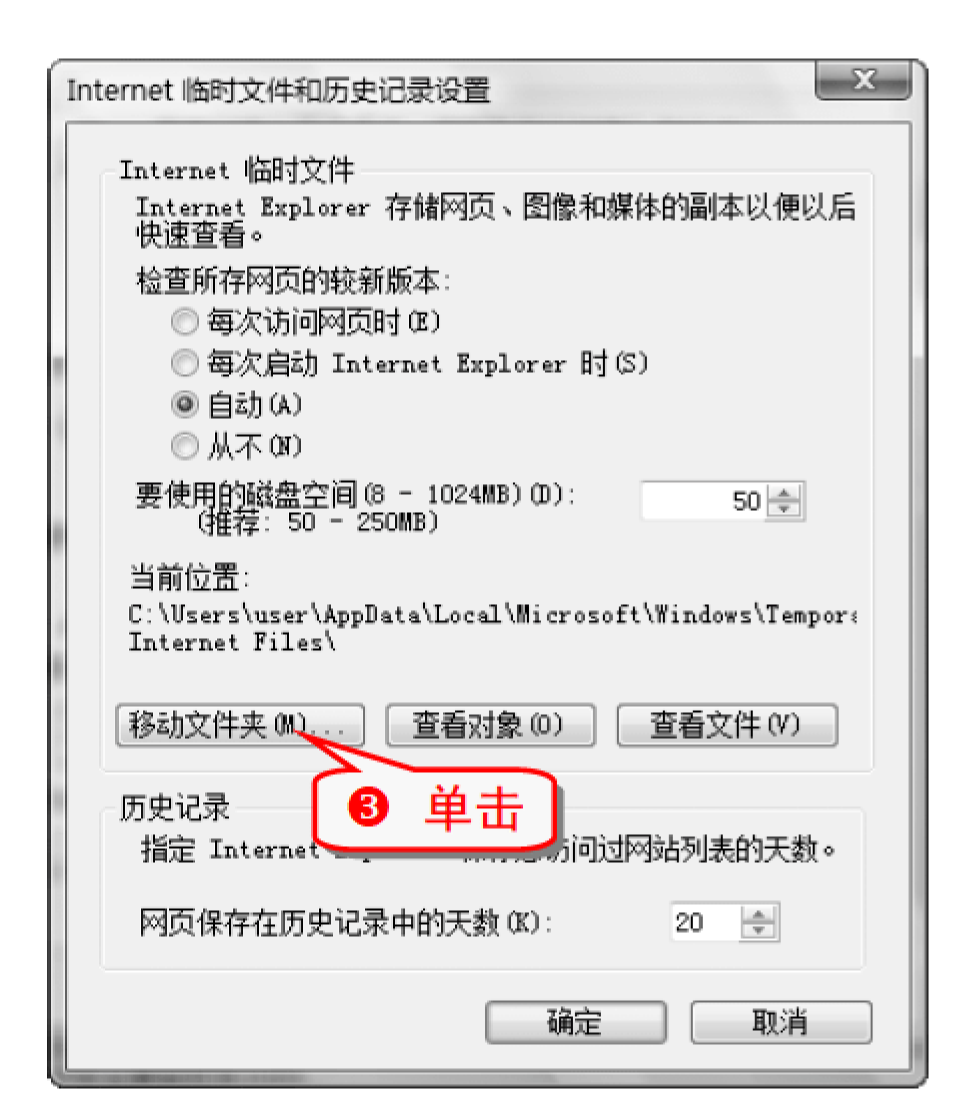
这样设置以后，也不能向收藏夹添加网址，否则会出错。

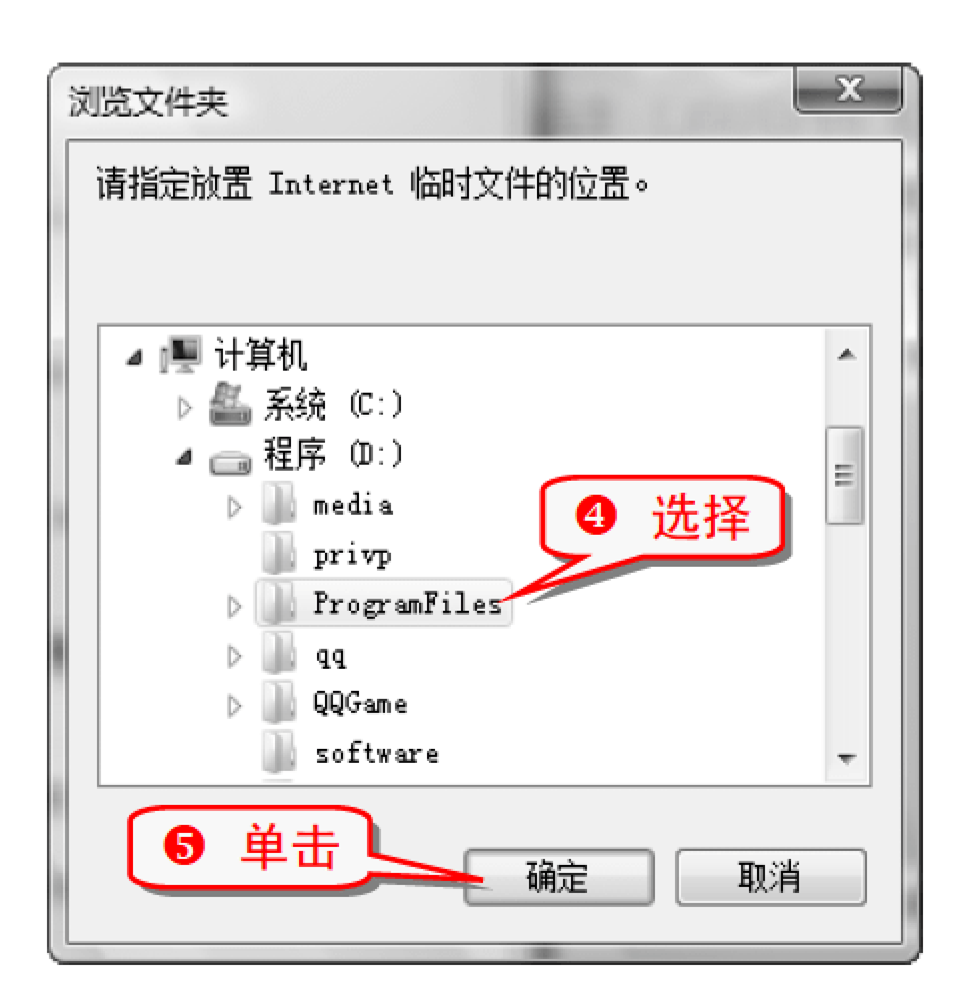
技巧54　给 IE 临时文件夹换位置

用 IE 上网时会将网上的部分文件保存在 C 盘一个默认的路径下，黑客很容易找到这个路径，为了安全着想，有必要给 IE 临时文件夹换个位置。

❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框。



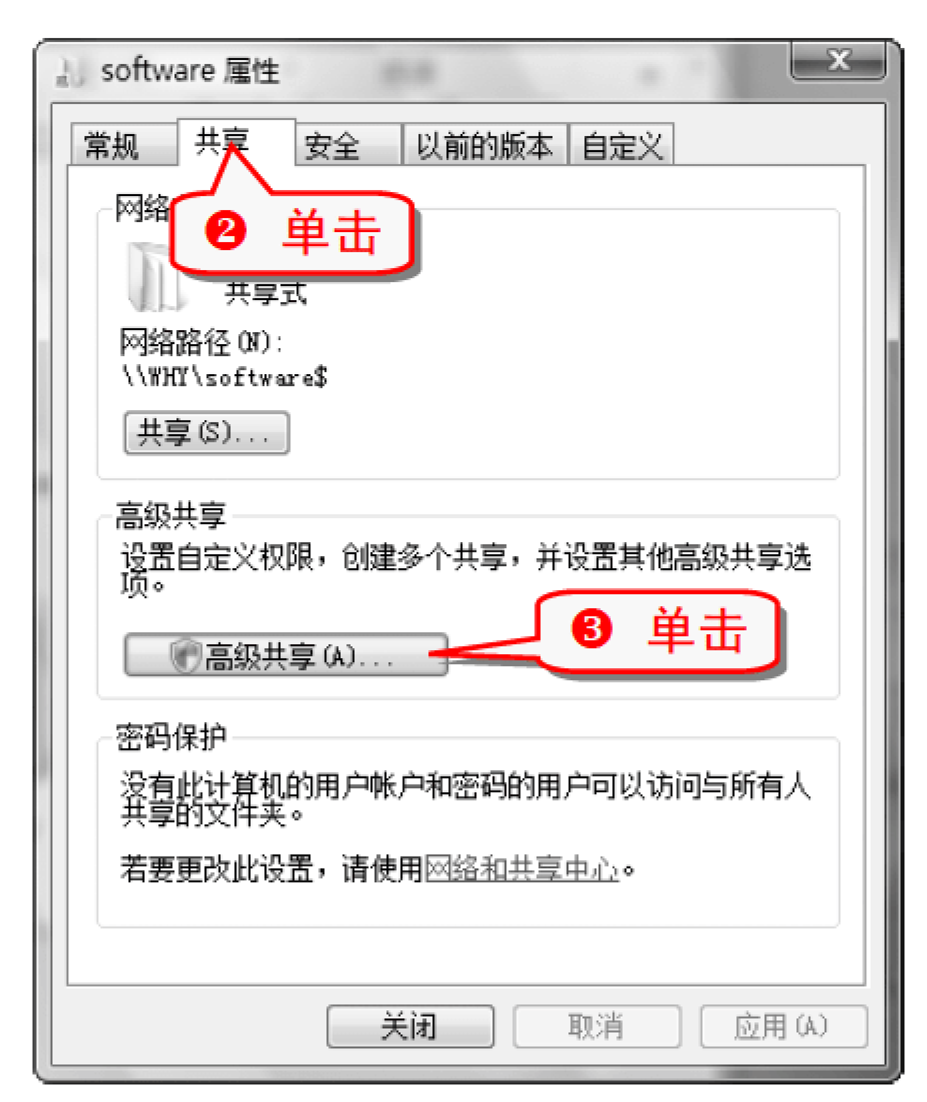




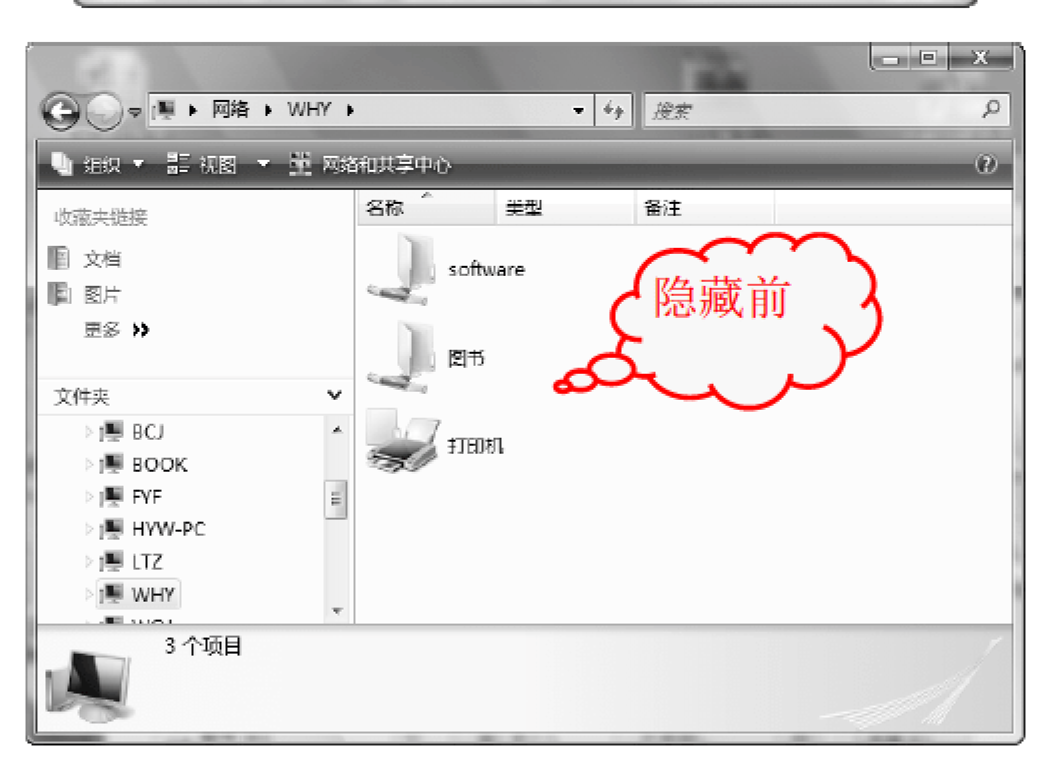
技巧55　在局域网中隐藏共享文件夹

在局域网中共享文件夹后，其他电脑可以从网络访问该共享文件夹。如果不想让陌生用户访问该文件夹，可以将其隐藏起来。

❶ 右击要隐藏的共享文件夹，在弹出的快捷菜单中选择“属性”命令。









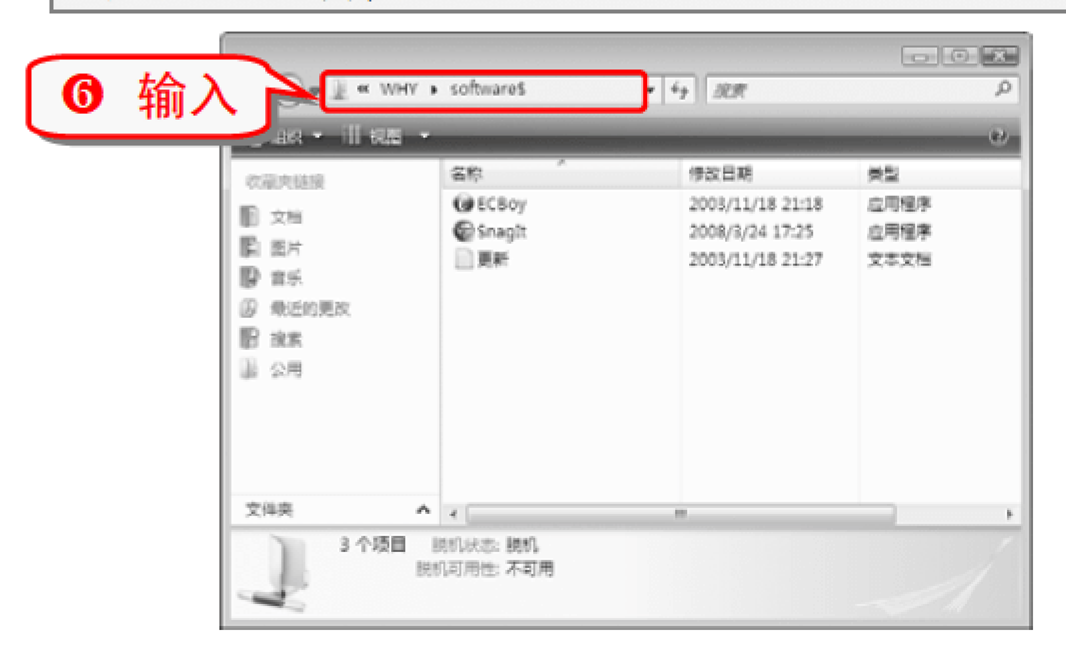
注 意 事 项

为共享文件夹修改共享名时，要先将其设置为不共享，再将其设置为共享，就可以将其改名了。否则共享名会显示为 software 而不能改名。

改名也只是在原文件名后面添加一个半角的“$”字符。

专 家 坐 堂

局域网的其他用户想要访问该共享文件夹时，只需输入“\\计算机名\software$”。



技巧56　在局域网中隐藏当前计算机

在局域网中不仅可以隐藏共享文件夹，也可以隐藏当前的计算机。

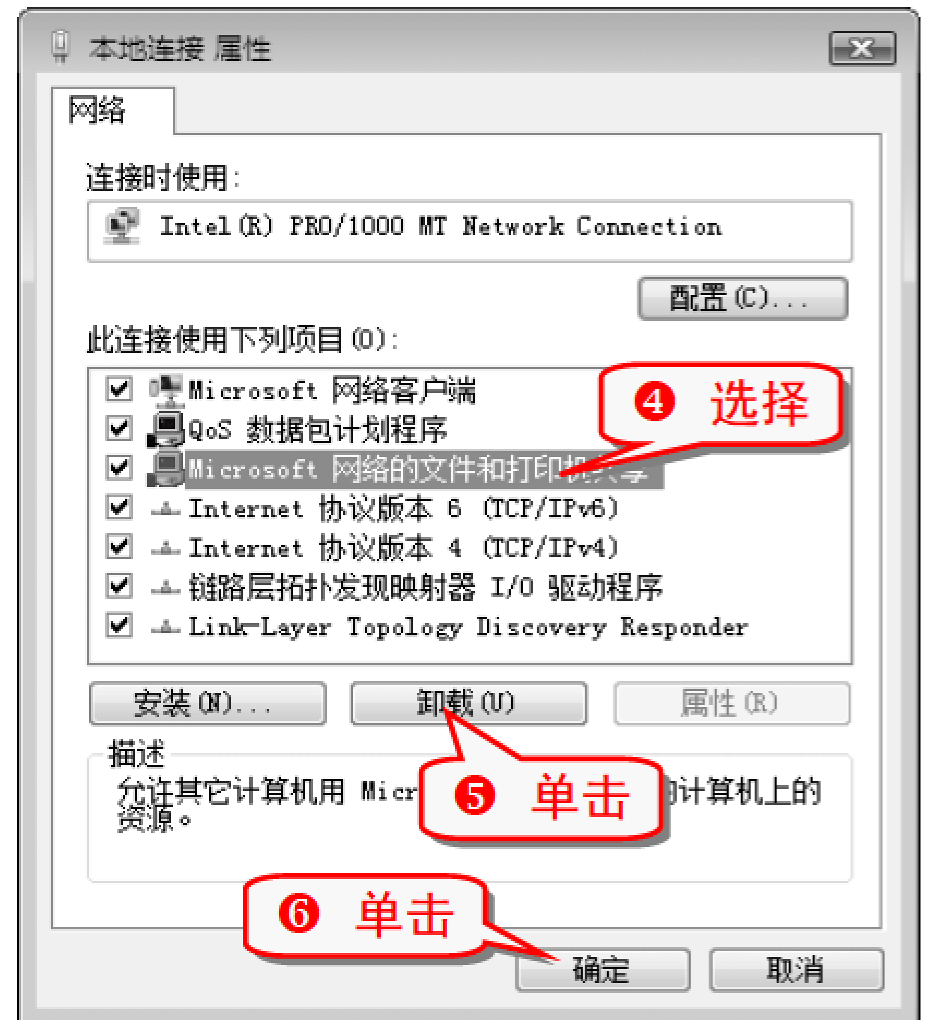
(1) 禁止访问当前电脑

❶ 右击“网络”图标，在弹出的快捷菜单中选择“属性”命令。

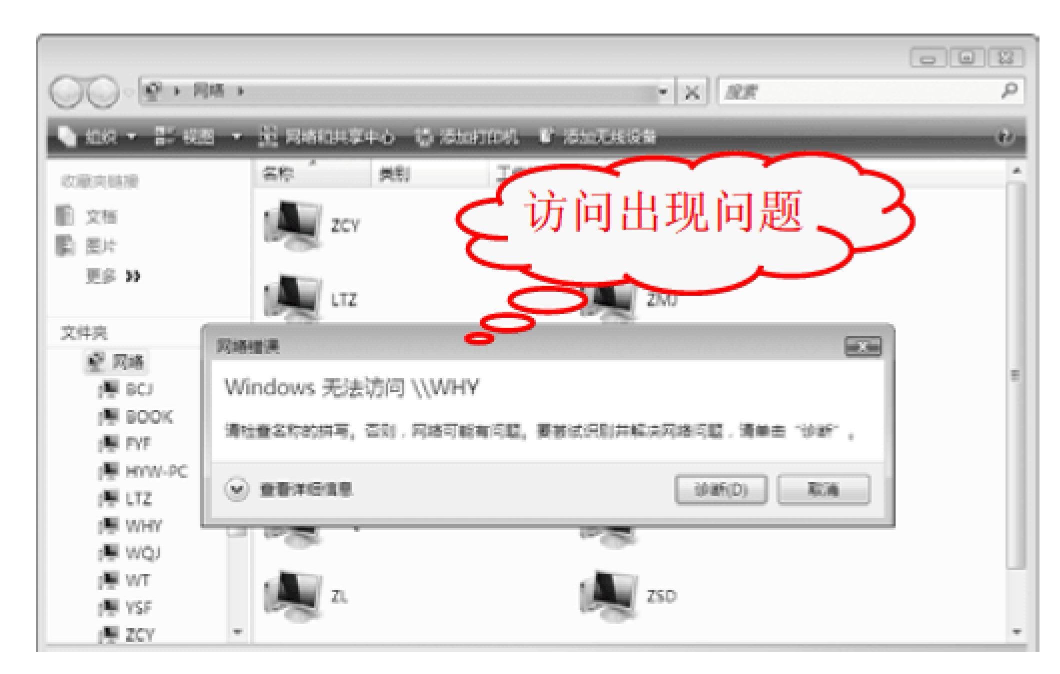








❼ 完成上述设置之后，在局域网中访问当前电脑时，将会弹出以下信息提示对话框。

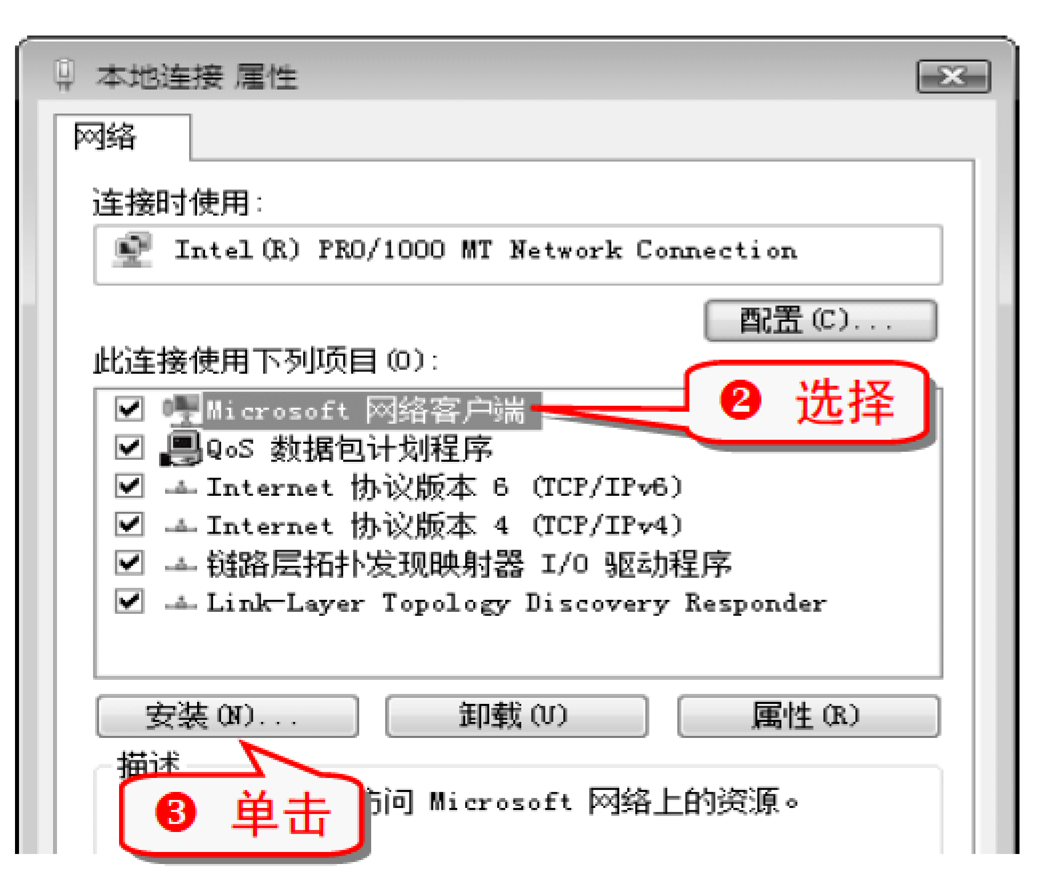


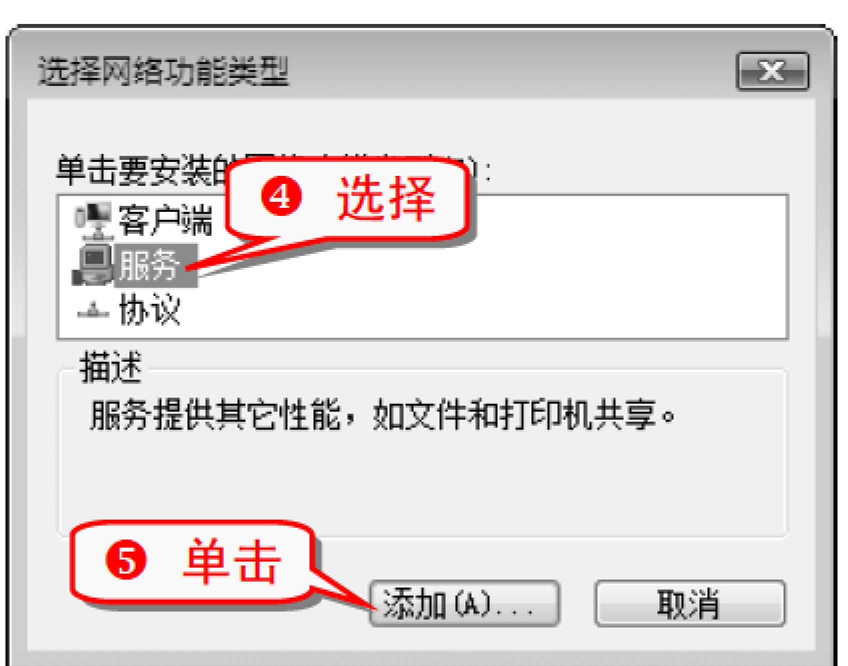
专 家 坐 堂

上述设置可以禁止局域网的其他用户访问当前电脑，但是在局域网内仍然可以看到该电脑。

(2) 取消禁止访问当前电脑

❶ 打开“本地连接 属性”对话框。





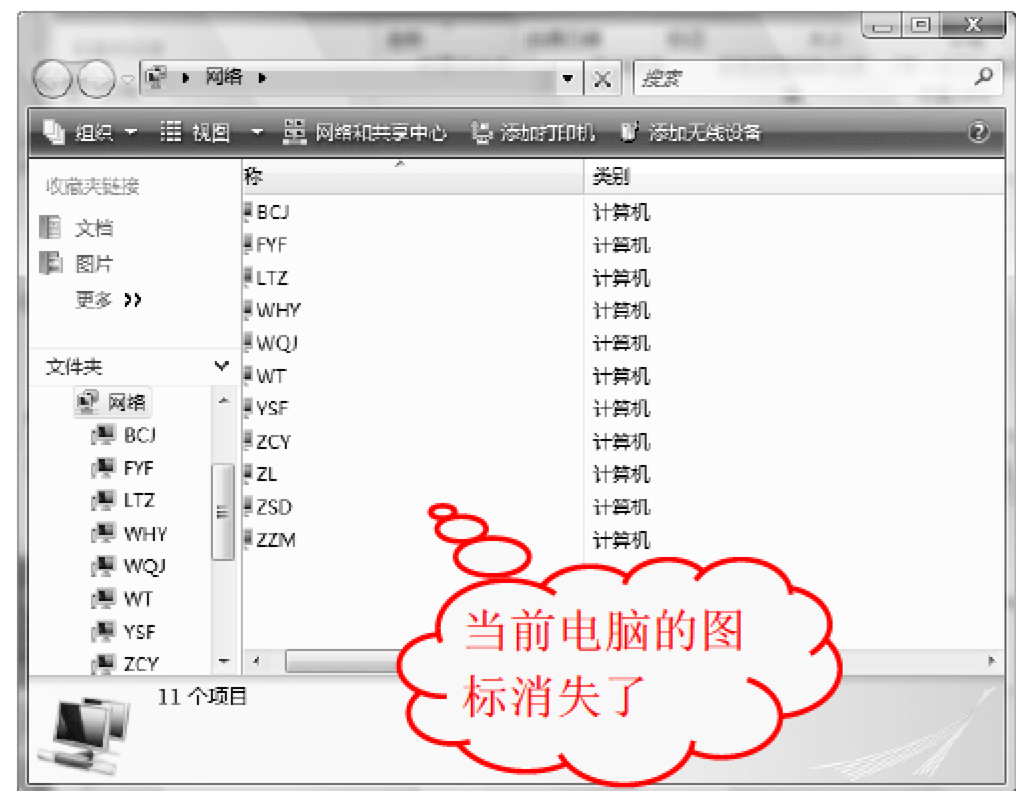


(3) 局域网中隐藏电脑图标

❶ 打开“网络和共享中心”窗口。







知 识 补 充

在第三个步骤中，选中“启用网络发现”单选按钮，就可以让当前电脑的图标在局域网中重新显示出来。

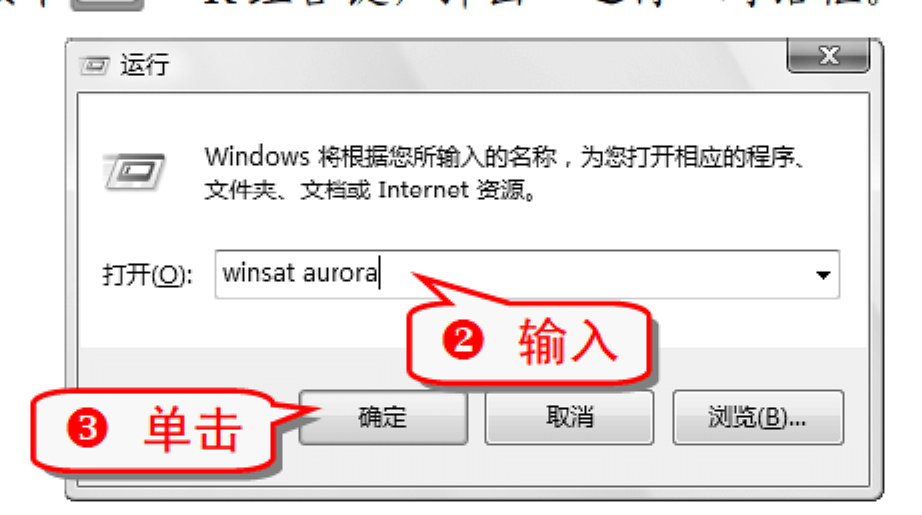
专 家 坐 堂

局域网的其他用户想要访问当前电脑时，只需输入“\\计算机名”。

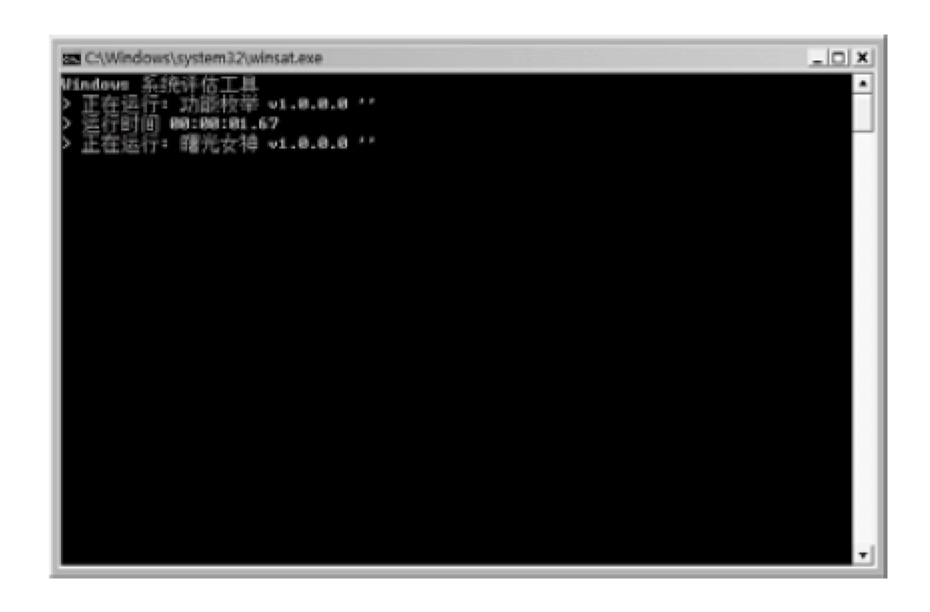
技巧57 使用动态屏保保护隐私

Windows Vista 系统中有一个 Windows XP 系统没有的功能，就是动态屏保。使用动态屏保功能也能起到保护隐私的效果。

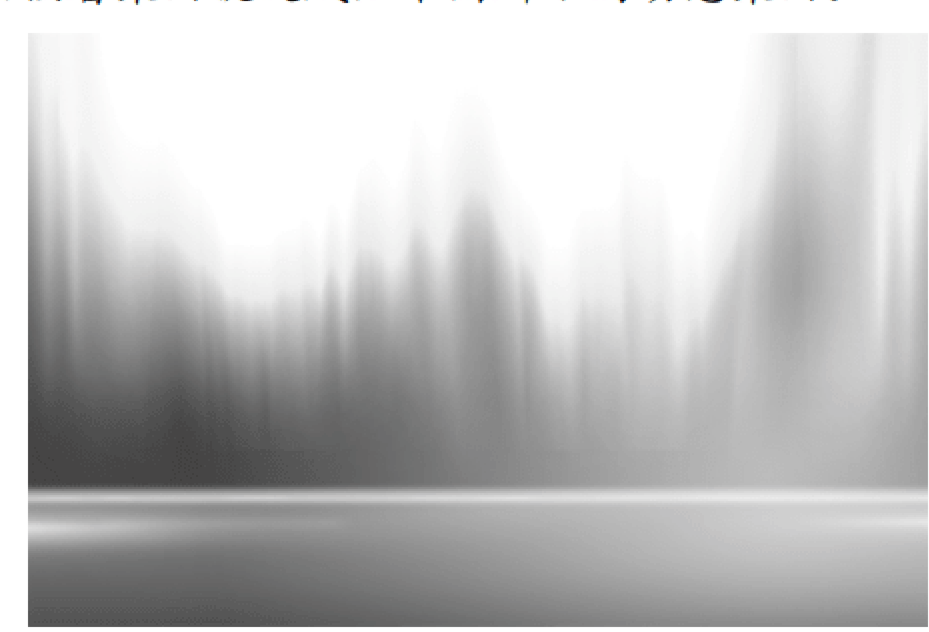
❶ 按下 ⊞ + R 组合键，弹出“运行”对话框。



❹ 桌面上会出现如下窗口。



❺ 紧接着桌面就变成如下图所示的动态桌面。



❻ 按下 Alt + Tab 组合键，调出任务切换窗口，按下 Esc 键可以退出动态桌面。

知 识 补 充

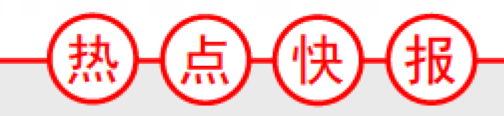
在全屏显示动态桌面的情况下，用鼠标点击桌面是没有任何反应的。



专题三 电脑加密无极限

内容导航

电脑中存放着很多商业机密文件和个人隐私文件，电脑一旦被黑客入侵，后果将不堪设想。需要对这些重要文件进行加密处理，这样才能保证用户利益不受损害。



- 设置开机密码
- 设置登录密码
- 设置密码安全策略
- 设置 Office 文档密码
- 加密可执行文件
- 加密 QQ 聊天记录

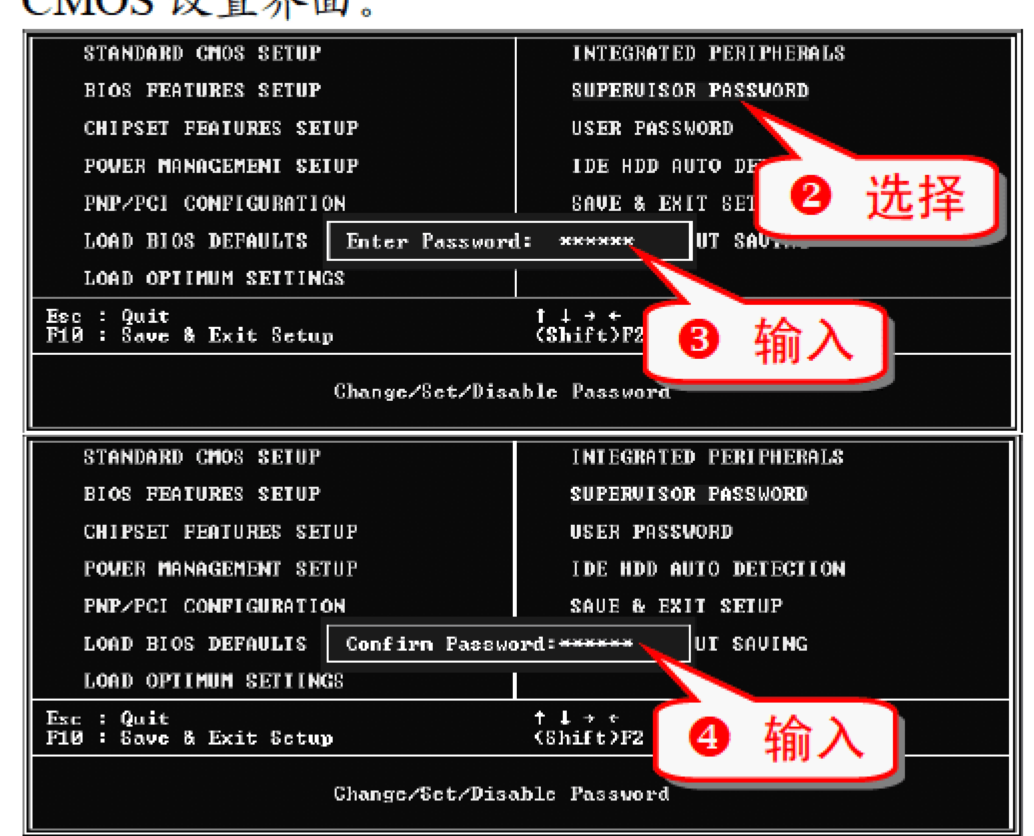
技巧58 设置开机密码

设置开机密码可以让别人无法进入系统，从而更有效地保护隐私。

(1) 设置超级用户密码

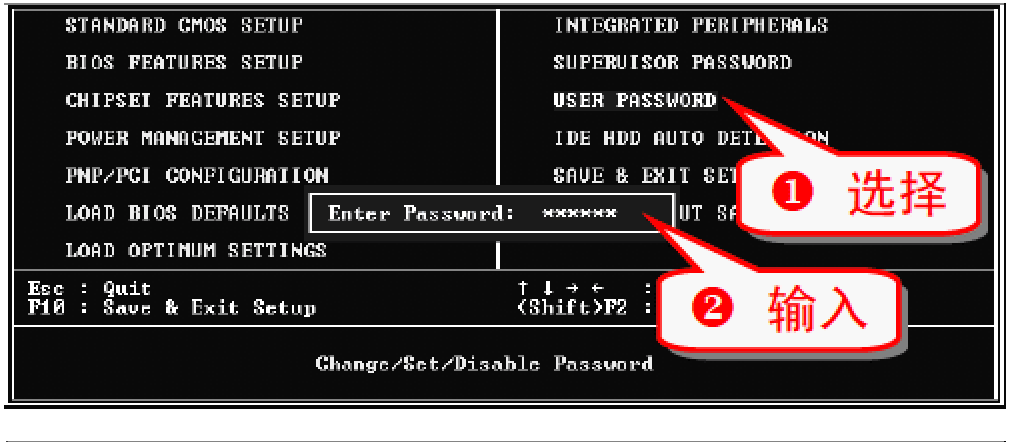
设置超级用户密码可以防止他人修改 BIOS 内容。

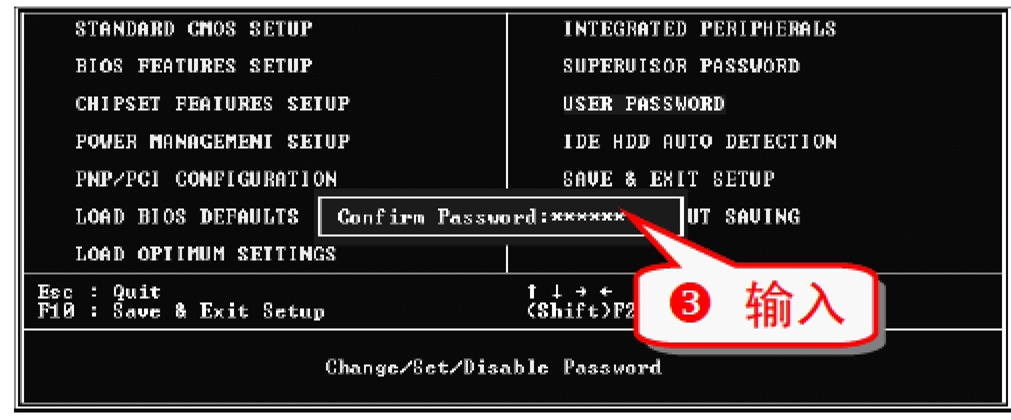
❶ 在电脑开机或重新启动的时候按下 Delete 键，进入 CMOS 设置界面。



(2) 设置用户密码

设置用户密码以后，在进入 BIOS 时输入正确的用户密码，能获得使用电脑的权限，但不能修改 BIOS 的设置。





(3) 让电脑开机检测密码

为电脑设置了 Supervisor Password 和 User Password 后，其作用是只在要进入 BIOS 设置界面时要求输入密码。通过以下的步骤可以让电脑在开机时就检测密码。







注 意 事 项

上述步骤是在 CMOS 模拟环境下进行的，CMOS 模拟程序可以从网上下载，容量很小。

对 BIOS 进行设置以后，不要忘记保存设置。



专 家 坐 堂

设置了超级用户密码和用户密码后，使用其中任意一个密码都能进入系统和 BIOS 设置界面，区别是通过用户密码进入 BIOS 设置界面后，不能修改里面的设置，但是能修改用户密码。

技巧59　设置登录密码

想要不通过 BIOS 设置开机密码，可以在系统里面设置用户登录的账户密码。

(1) 设置登录密码

❶ 选择"开始"→"控制面板"命令，弹出"控制面板"窗口。

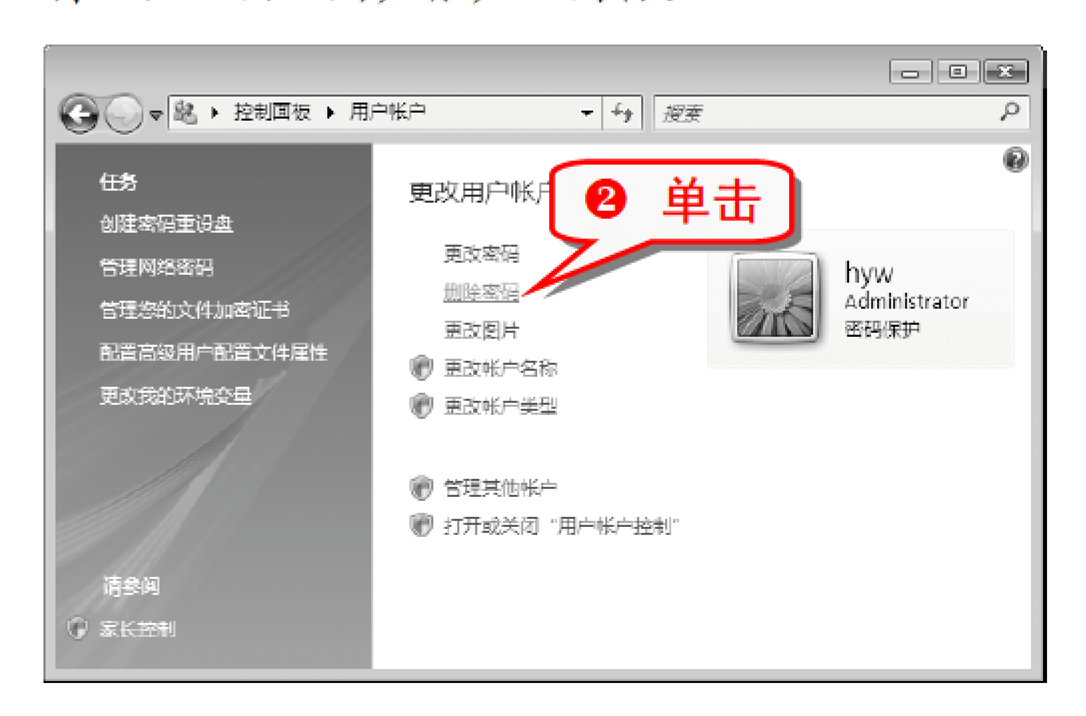






(2) 删除登录密码

❶ 选择"开始"→"控制面板"命令，弹出"控制面板"窗口，双击"用户帐户"图标。







专 家 坐 堂

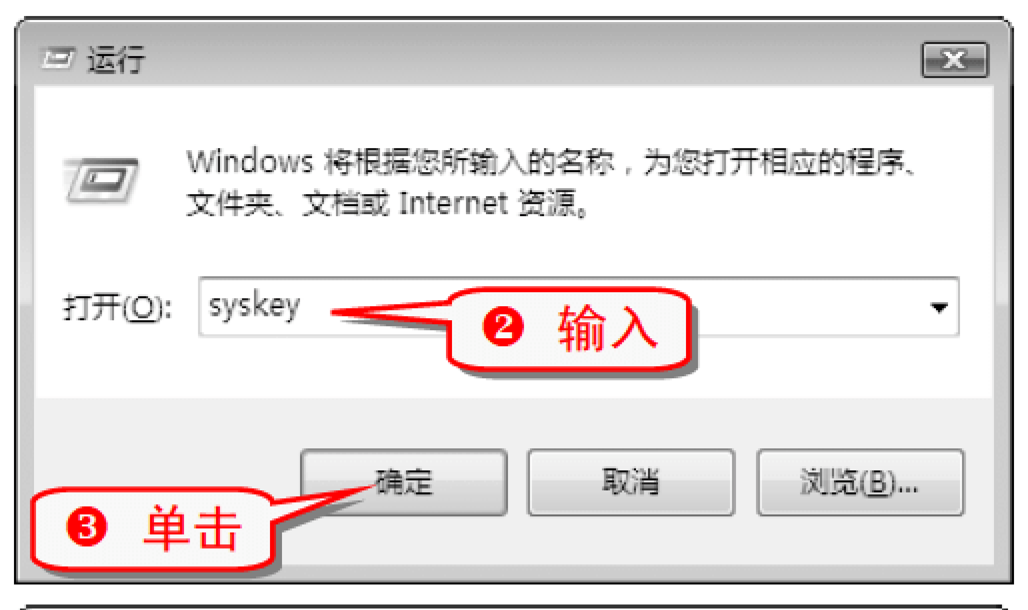
密码复杂度越强，就越能保护电脑免受黑客侵害。在选择密码的时候最好选择强密码。强密码的长度至少有 8 个字符，不包括用户名、真实姓名或公司名称，不包括完整的单词，要包含大写字母、小写字母、数字以及键盘上的符号。

技巧60　设置超强的启动密码

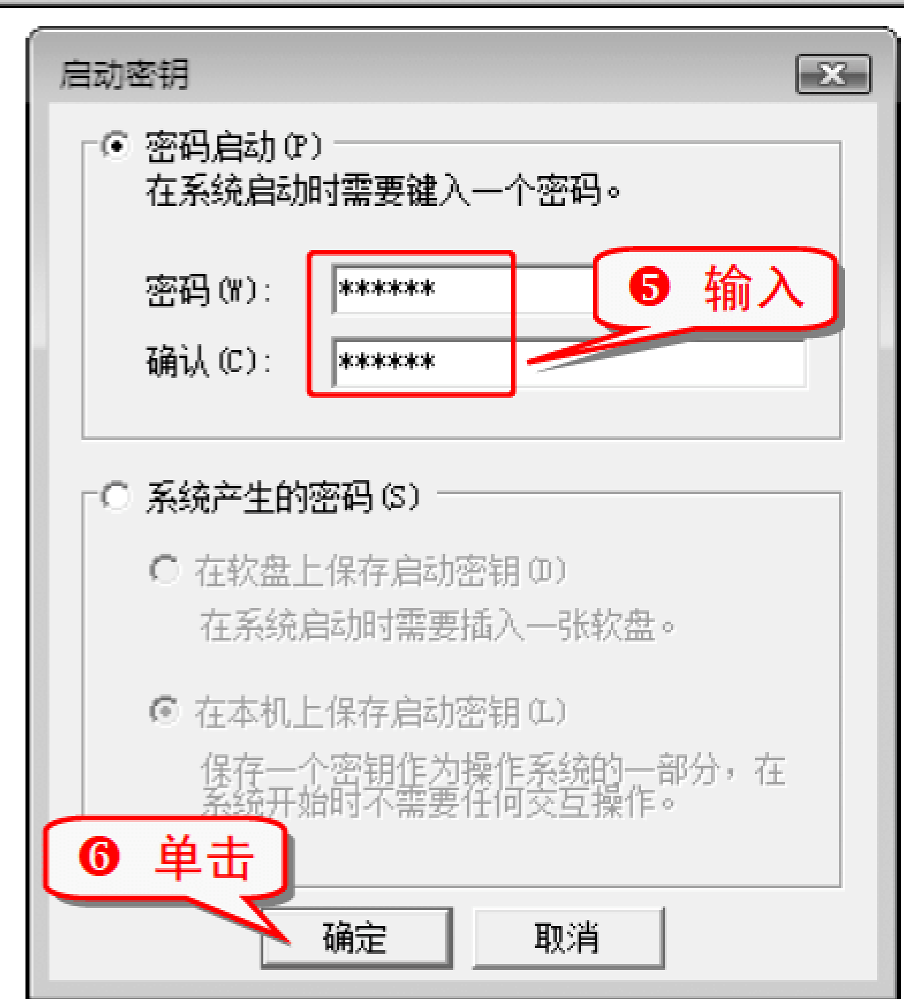
对于 Windows Vista 而言，除了可以设置登录密码，还可以设置超强的启动密码。

❶ 按下 ⊞ + R 组合键，打开"运行"对话框。











❽ 重新启动后电脑后出现如下对话框。



专　家　坐　堂

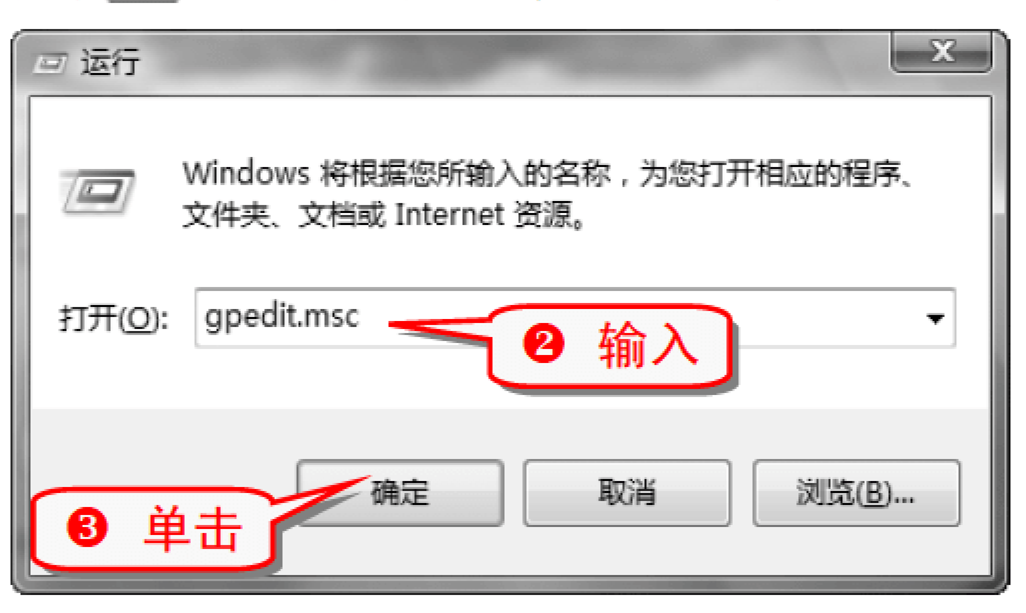
如果需要取消系统启动密码，可以在“启动密钥”对话框中选中“系统产生的密码”选项组中的“在本机上保存启动密钥”单选按钮，系统重新启动后就不会出现“启动密码”对话框了。

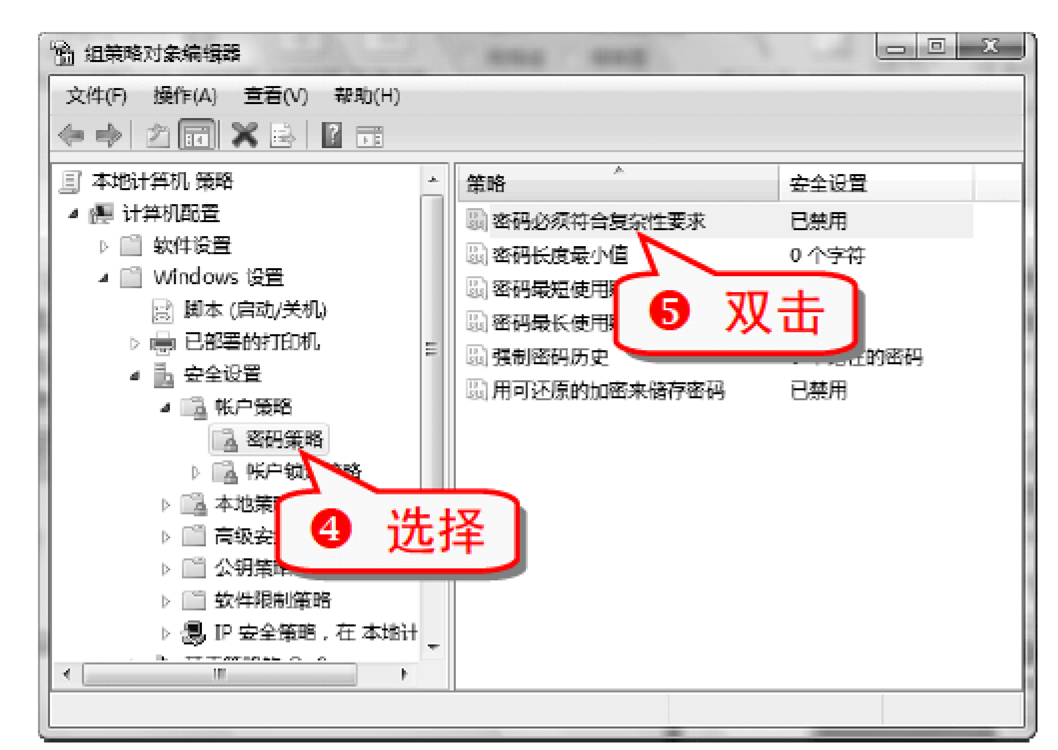
技巧61　增强设置密码复杂度

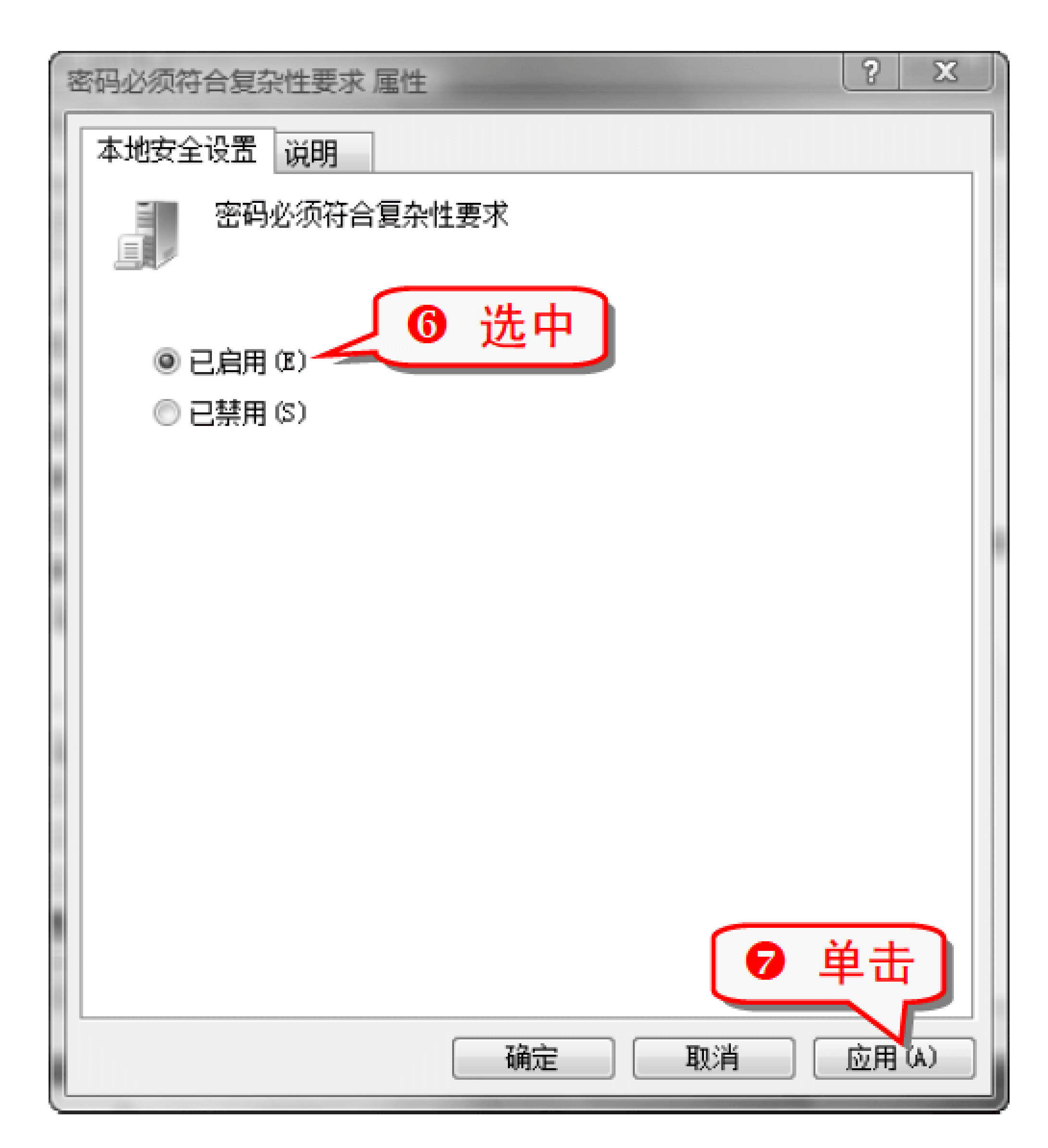
在设置密码时为了便于记忆，通常都选择容易记的密码，通过以下几步设置后，可以让 Windows Vista 的密码设置符合要求。

(1) 设置密码复杂度

❶ 按下 ⊞ + R 组合键，打开“运行”对话框。



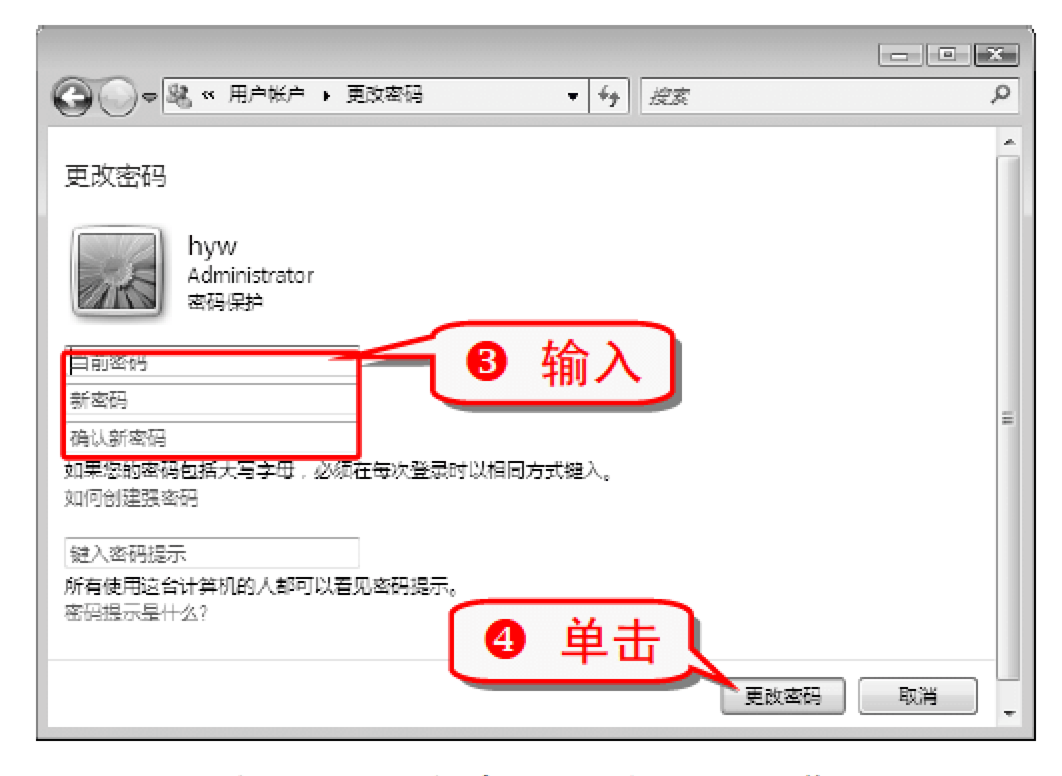




(2) 测试设置效果

❶ 选择"开始"→"控制面板"命令，在弹出的"控制面板"窗口中双击"用户帐户"。





❺ 如果输入密码过于简单，则弹出如下警告框。



专 家 坐 堂

测试过程中可以发现，如果输入的密码过于简单是不能设置成功的，必须输入强密码，才能设置成功。而且在这种情况下不能进行删除用户密码的操作。

技巧62 限制密码输入次数

为避免猜测密码的事情发生，可以设置密码的输入次数限制。

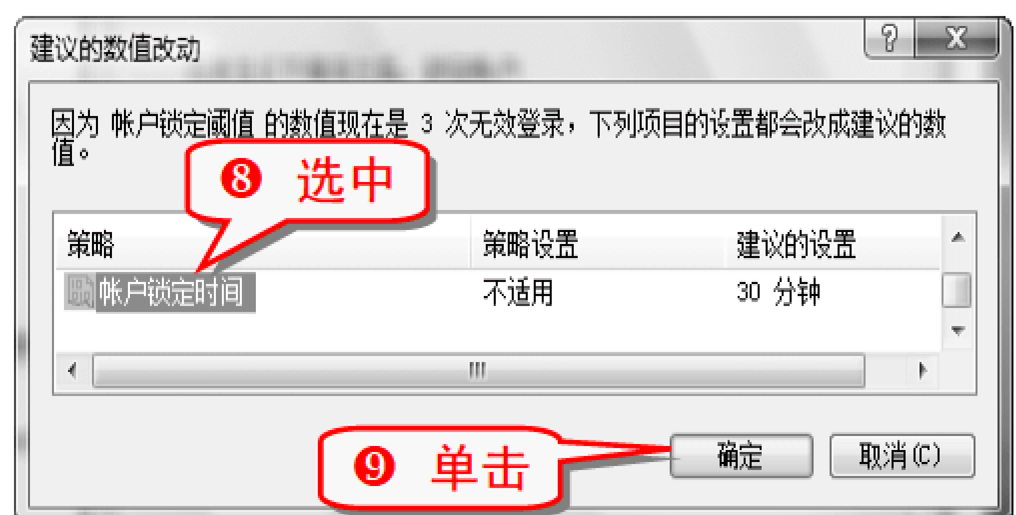
❶ 按下⊞+R组合键，打开"运行"对话框。











注　意　事　项

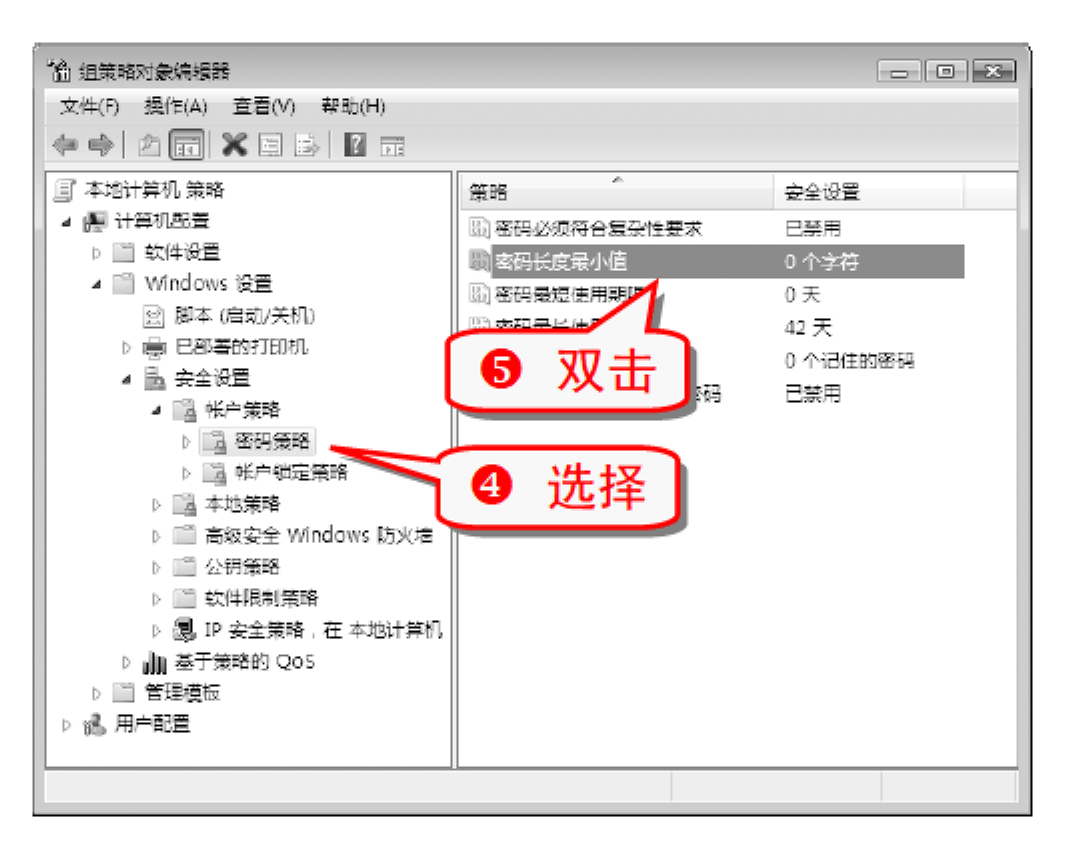
一定要记住登录密码，否则三次密码输入错误，就会将电脑锁定，30 分钟内任何人都无法进入系统。

技巧63　限制密码输入长度

为电脑设置密码输入的长度限制，使得在设置密码时不得不输入比较长的密码，这样有利于系统的安全。

❶ 按下 [Win] + R 组合键，打开“运行”对话框。







❽ 如果设置长度小于 8 的密码就会出现下面这种提示对话框。

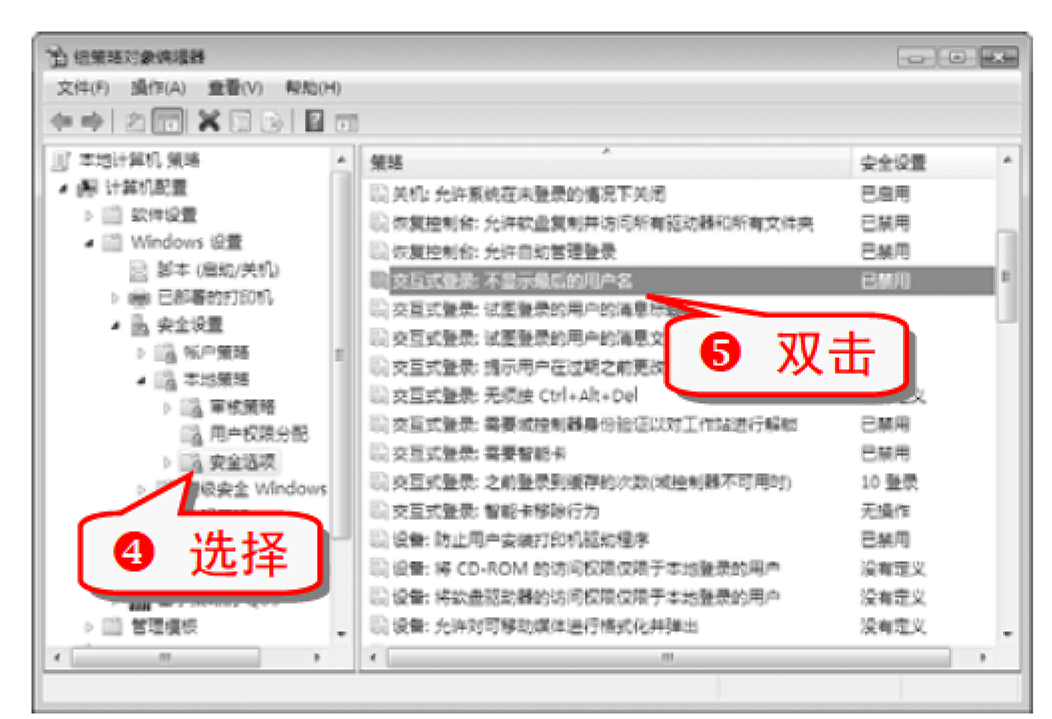


技巧64　为 Windows Vista 设置账户保密

默认情况下，Windows Vista 系统下的登录框中会保留上次登录的用户名。要做到账户保密，可以隐藏上次登录的账户。

❶ 按下 ⊞ + R 组合键，打开“运行”对话框。







❽ 重新启动电脑后，发现用户名一栏为空。



技巧65　设置电源管理密码

Windows Vista 操作系统中有设置电源管理密码的功能，可以为电脑的“挂起”状态设置密码，不知道密码就无法让电脑从“挂起”状态返回到正常状态。

❶ 选择“开始”→“控制面板”命令，弹出“控制面板”窗口。









注 意 事 项

电源管理的密码是用户的登录密码，如果没有设置用户登录密码，必须先对其进行设置，才能使用电源管理密码功能。

技巧66 设置屏幕保护程序密码

在短时间内要离开电脑，但又不愿意把电脑关掉的情况下，可以使用屏幕保护程序密码，让电脑避免被查看。

❶ 右击桌面上的空白处，在弹出的快捷菜单中选择“个性化”命令，打开“个性化”窗口。





注 意 事 项

屏幕保护密码使用的是用户登录的密码，这一点跟电源管理密码是一样的。

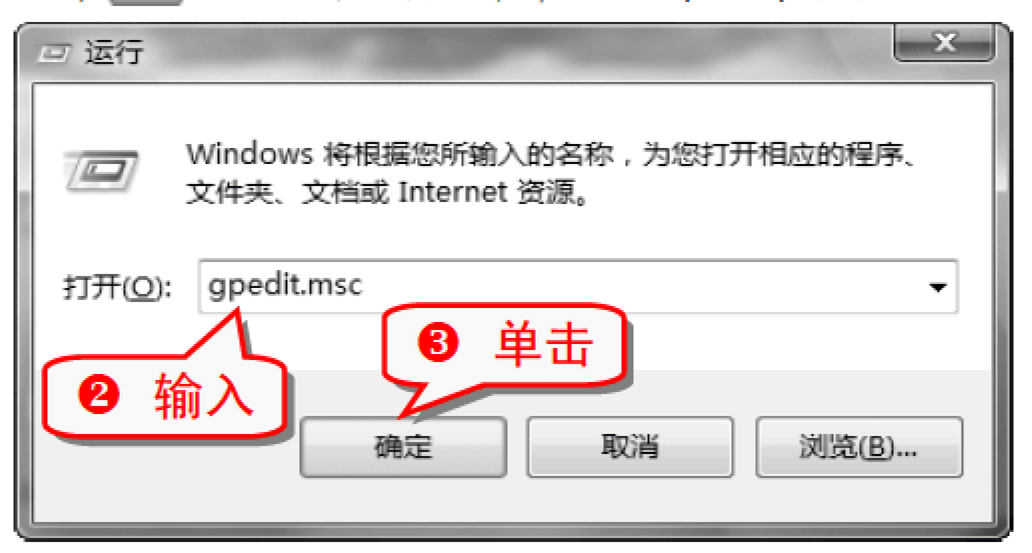
知 识 补 充

电源管理的密码是用户登录密码，如果没有设置用户登录密码，必须先对其进行设置，才能使用电源管理密码功能。

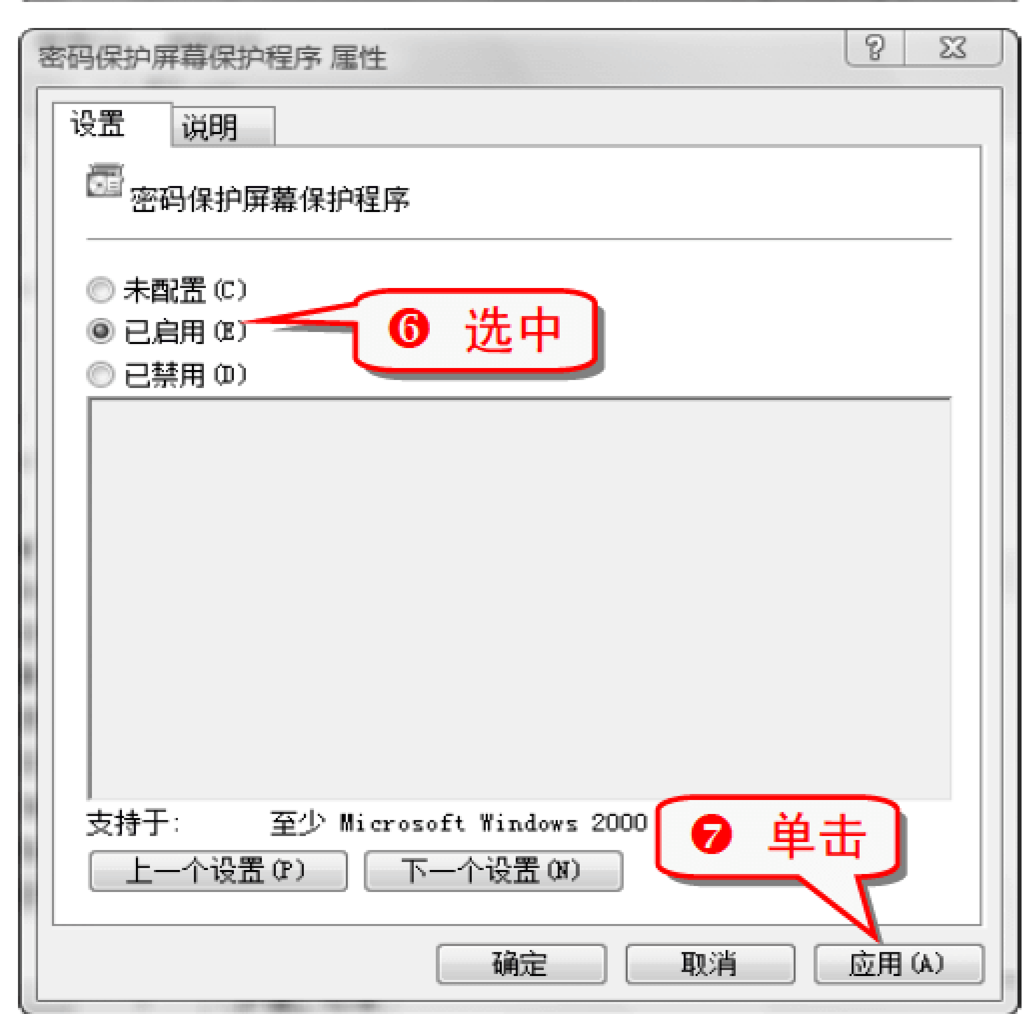
技巧67 为所有屏幕保护程序设置密码

通过设置组策略对象编辑器，可以为所有的屏幕保护程序设置密码。

❶ 按下 ⊞ +R 组合键，打开“运行”对话框。







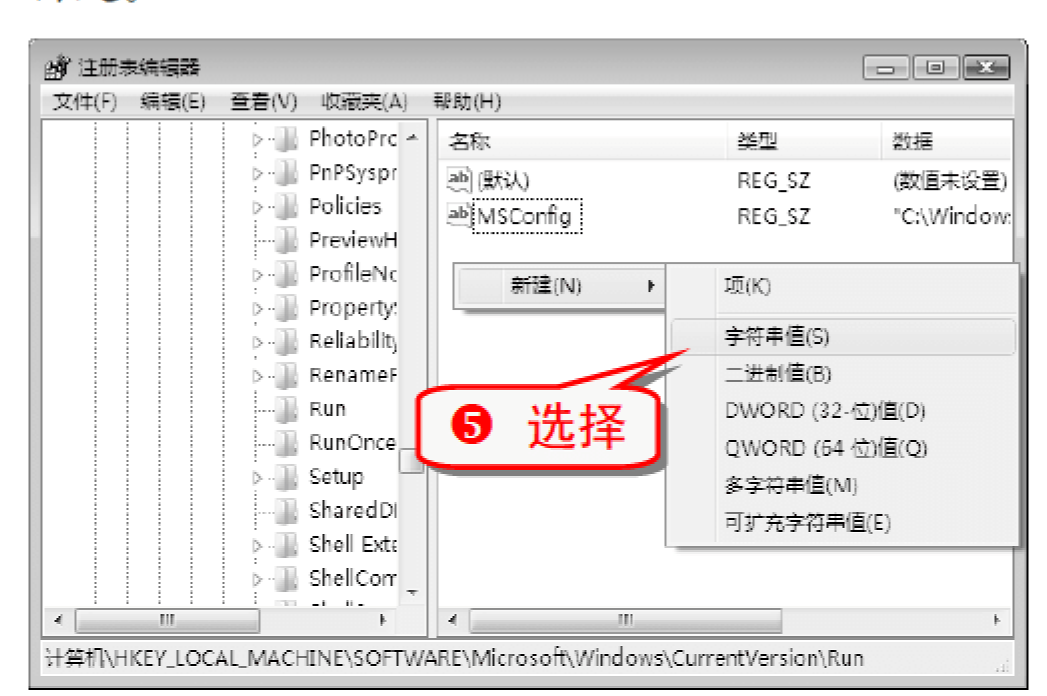
技巧68　让电脑开机后立即运行屏幕保护程序

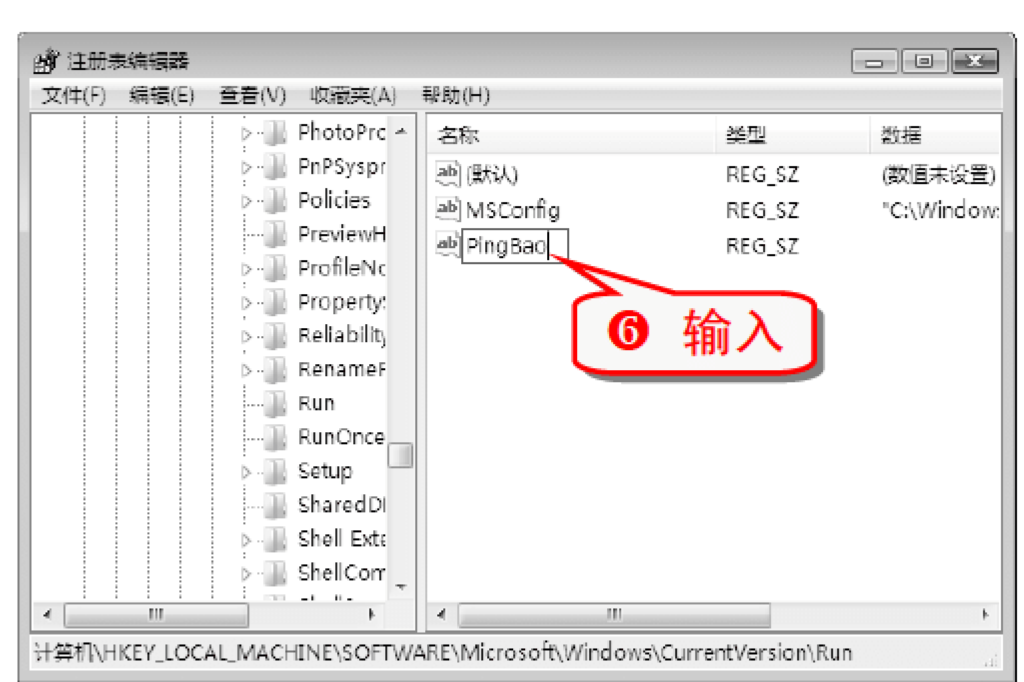
通过修改注册表，可以让电脑在开机后立即运行屏幕保护程序。

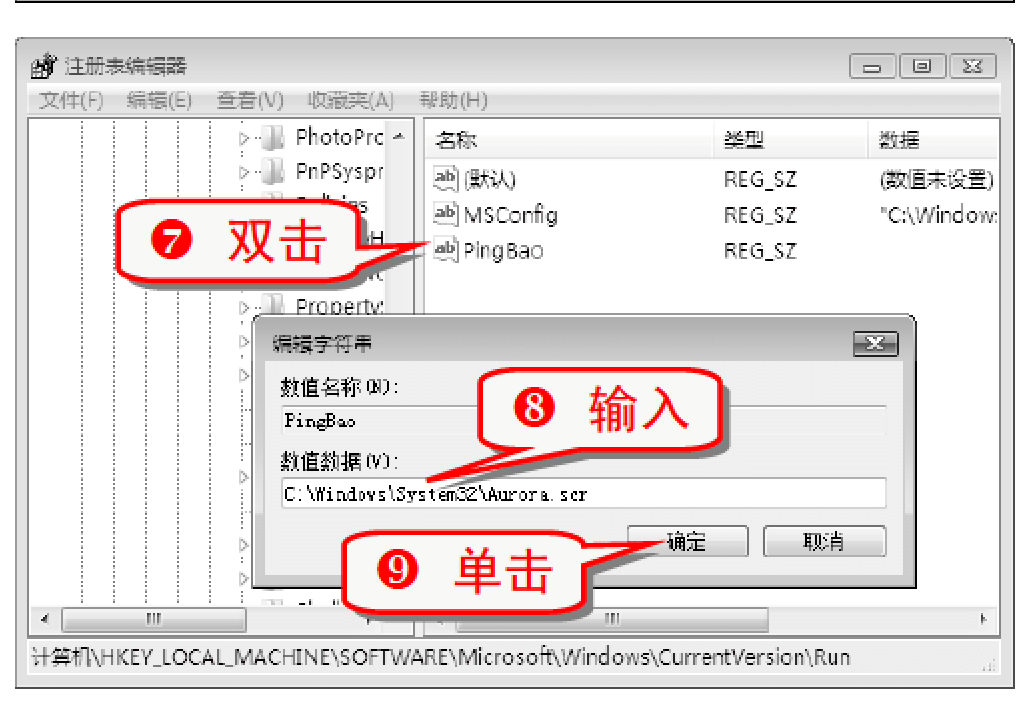
❶ 按下 ⊞ + R 组合键，打开“运行”对话框。



❹ 展开 HKEY-LOCAL-MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 分支，右击右边窗格的空白处。









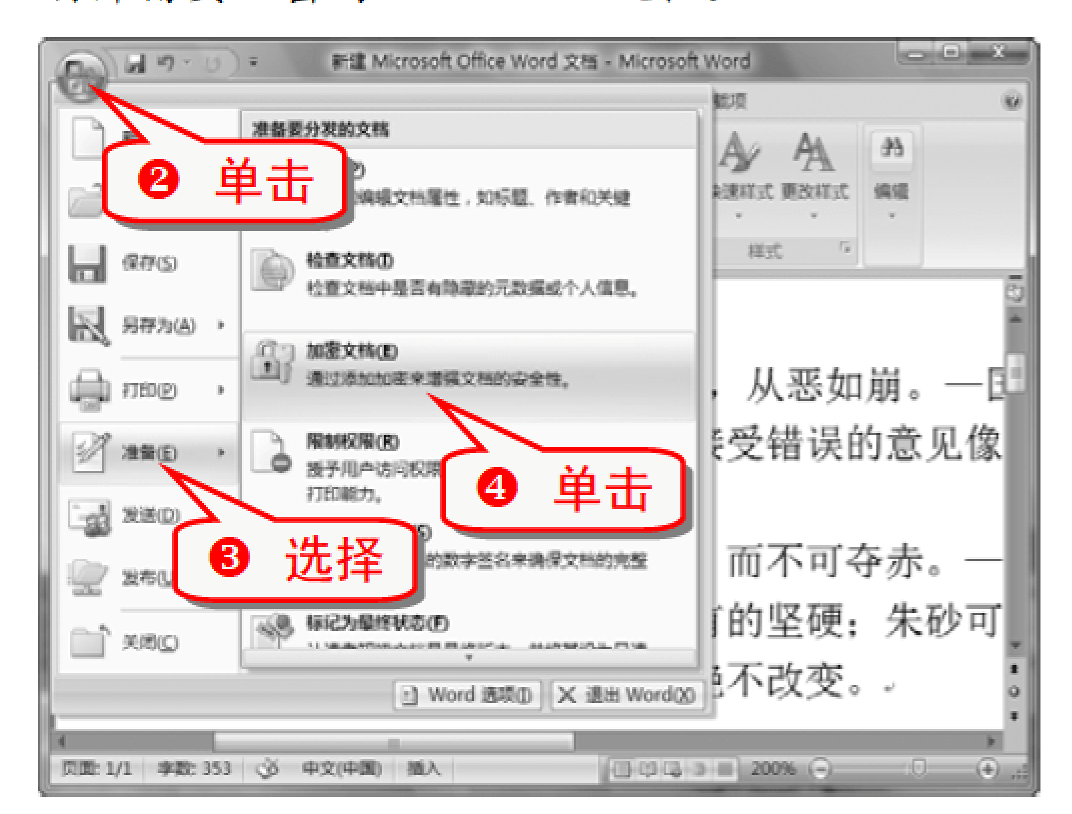
注 意 事 项

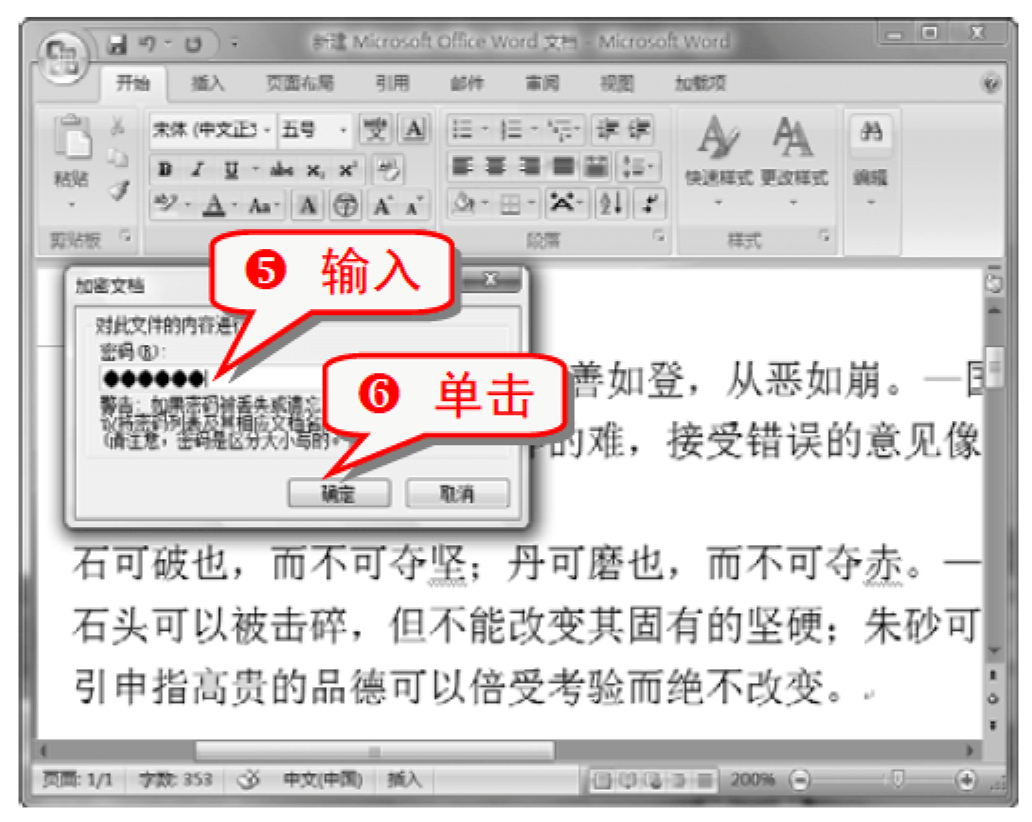
重新启动或注销电脑后，就可以看到设置效果。PingBao 的数值可以设置为其他的屏幕保护程序。

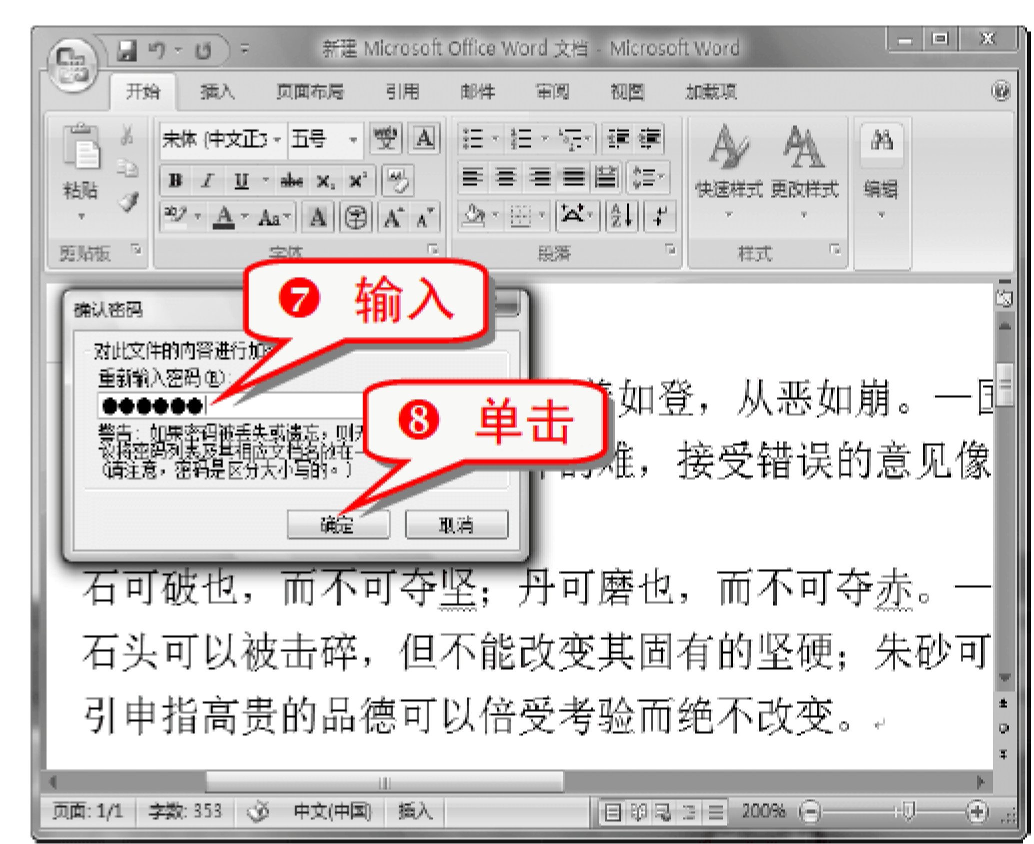
技巧69　为 Word 2007 文档设置密码

在 Word 2007 中，如果不想让别人看到文档的内容，可以对文档设置访问密码，只有密码输入正确才能访问文档。

❶ 打开需要加密的 Word 2007 文档。











注 意 事 项

虽然对文件进行了加密，但是在不知道密码的情况下还是可以对文件进行删除操作。

技巧70 利用宏命令自动加密 Word 2007 文档

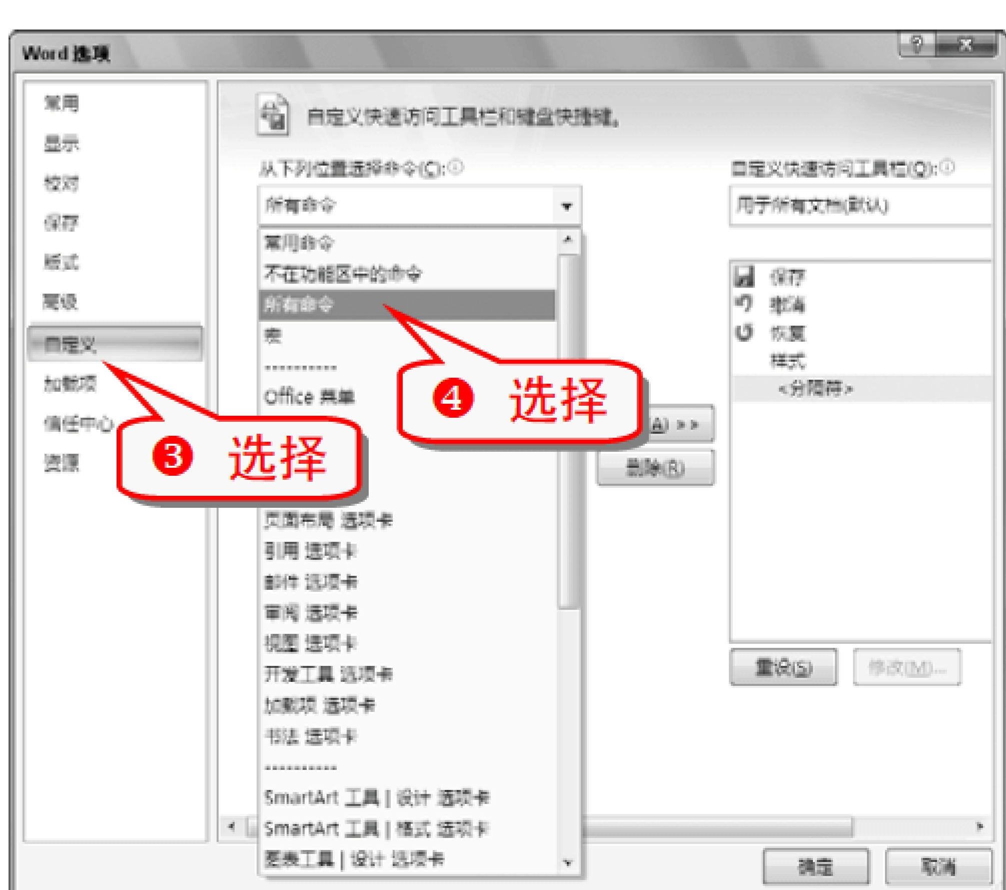
在 Word 2007 中利用宏命令可以快速实现文档的加密操作。

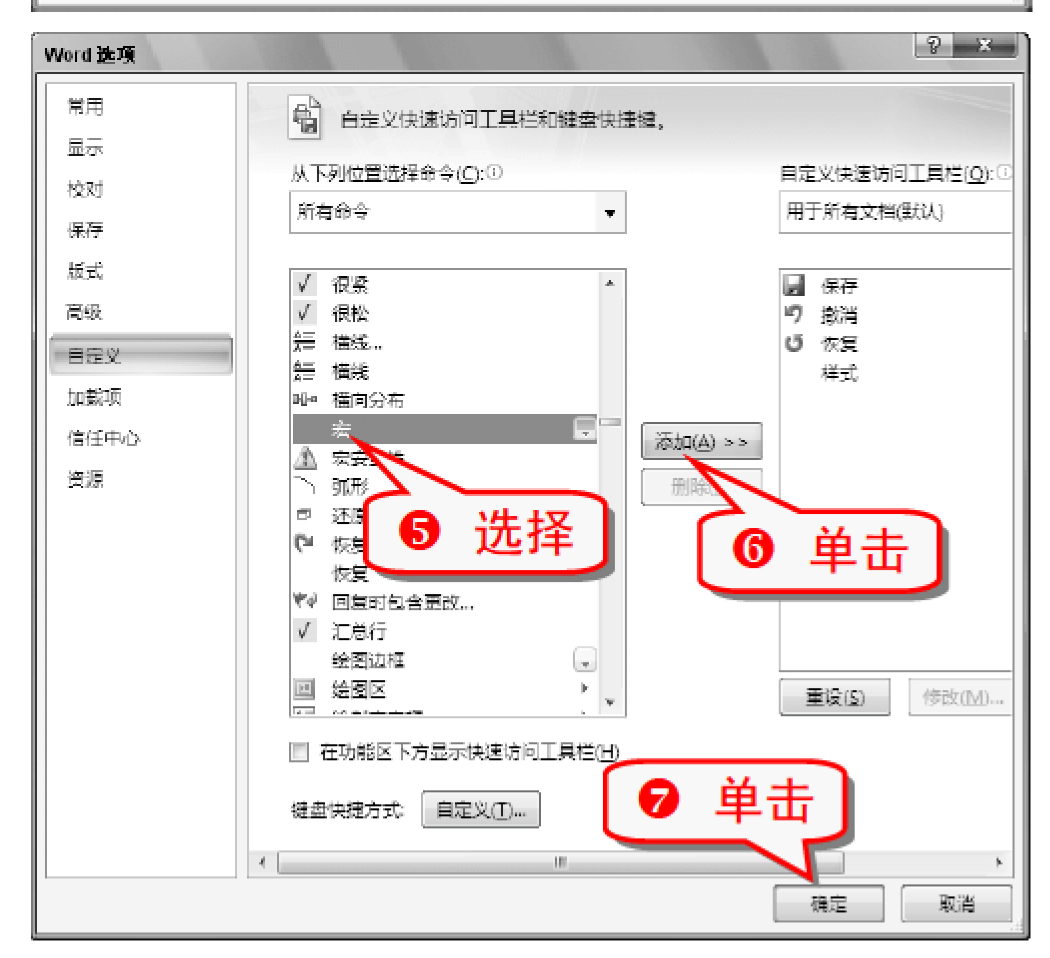
(1) 添加宏命令的快捷访问工具栏

将宏添加到“自定义快速访问工具栏”中，可以方便使用宏命令。

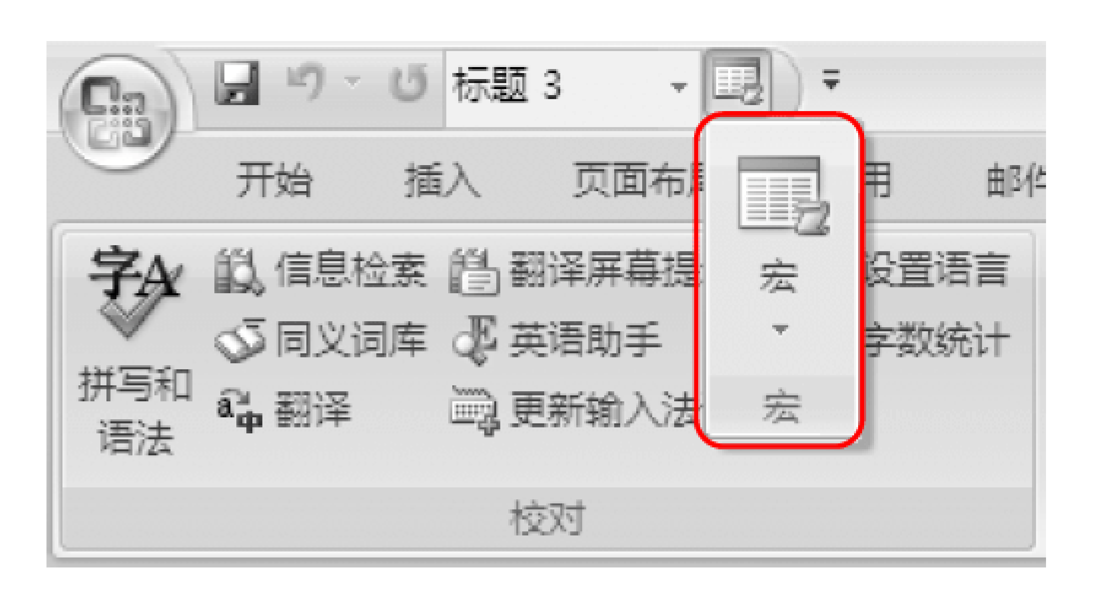
❶ 单击 Office 按钮，弹出 office 菜单。







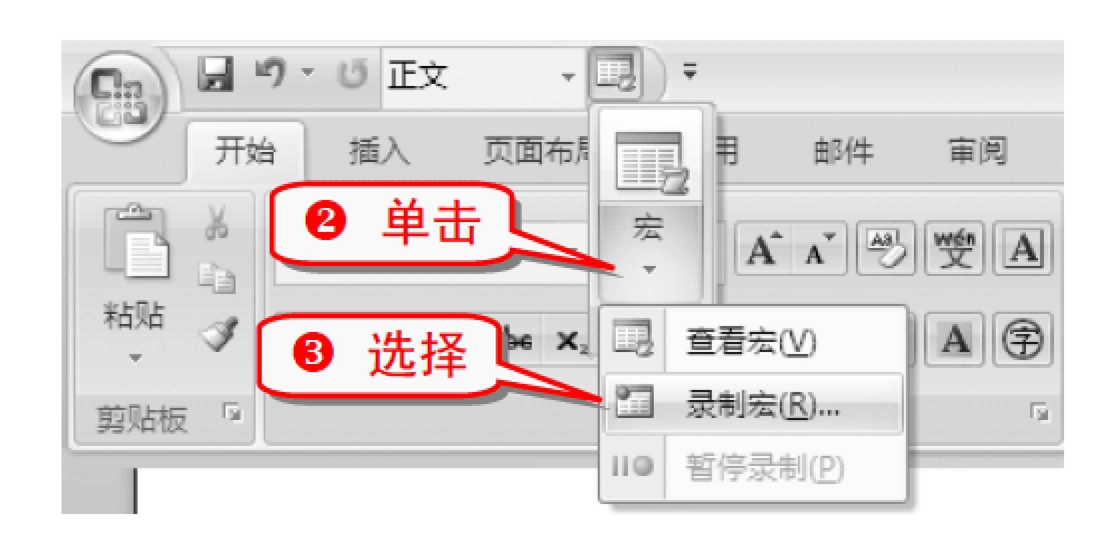
❽ “宏”命令按钮出现在“自定义快速访问工具栏”中。



(2) 录制宏

将“宏”命令添加到“自定义快速访问工具栏” 后，即可录制宏命令。

❶ 单击“自定义快速访问工具栏”中的“宏”命令。



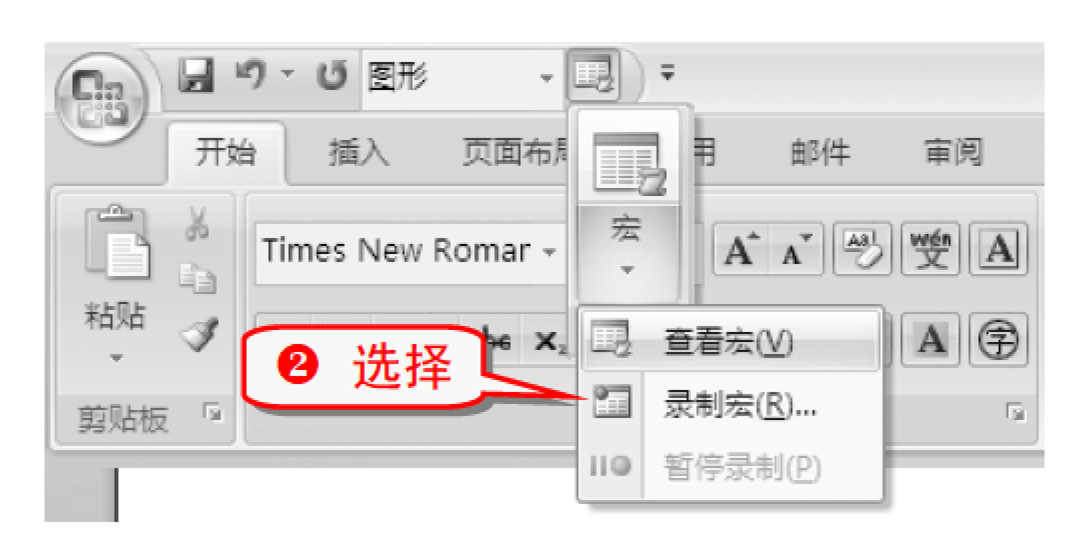






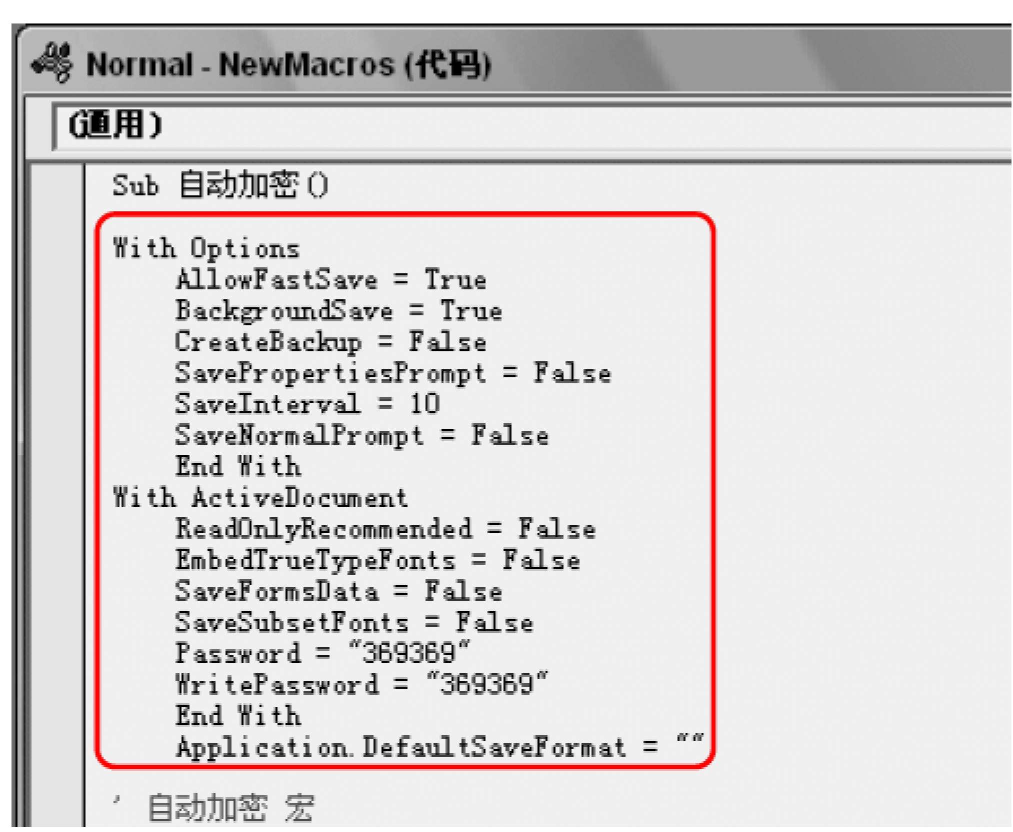
(3) 对宏命令进行编辑

❶ 单击“自定义快速访问工具栏”中的“宏”命令。





❹ 在弹出的“Normal-NewMacros(代码)”对话框中输入代码。





举 一 反 三

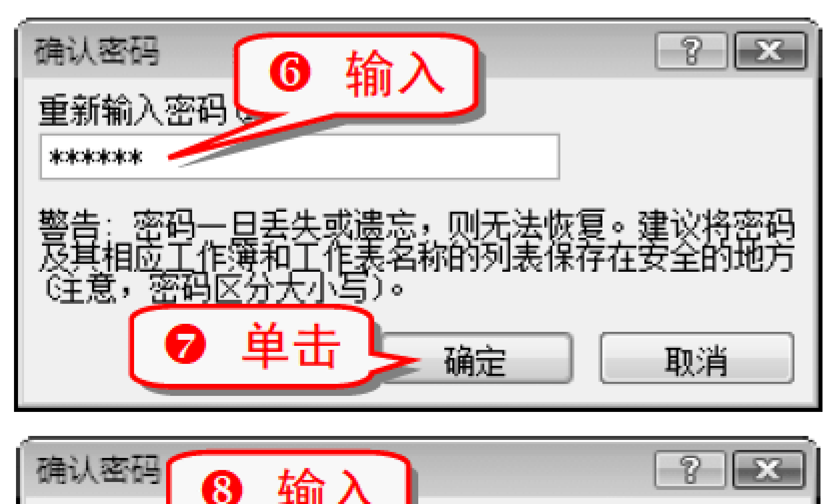
“PassWord=”和“WritePassword=”后面跟的密码分别表示打开文件时需要的密码和修改文件时需要的密码。

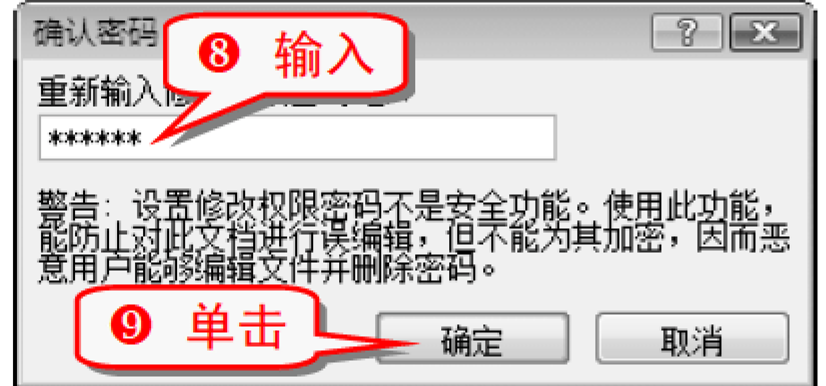
技巧71 为 Excel 2007 文档设置密码

对 Excel 2007 文档进行加密的步骤如下。

❶ 选择“Office 按钮”→“另存为”命令，弹出“另存为”对话框。









知　识　补　充



可以在“常规选项”对话框中对工作簿设置“只读”方式。选中单选按钮“建议只读”即可。当打开文件时，会弹出对话框询问是否以只读方式打开文件。设置“只读”方式可以对只读文件进行读取或复制。如果对只读文件进行了更改，则只能将文件另外进行保存。

举　一　反　三

Word 文档加密的方法同样适用于 Excel 文档，完全可以按照前面给 Word 文档加密的方法给 Excel 文档加密。

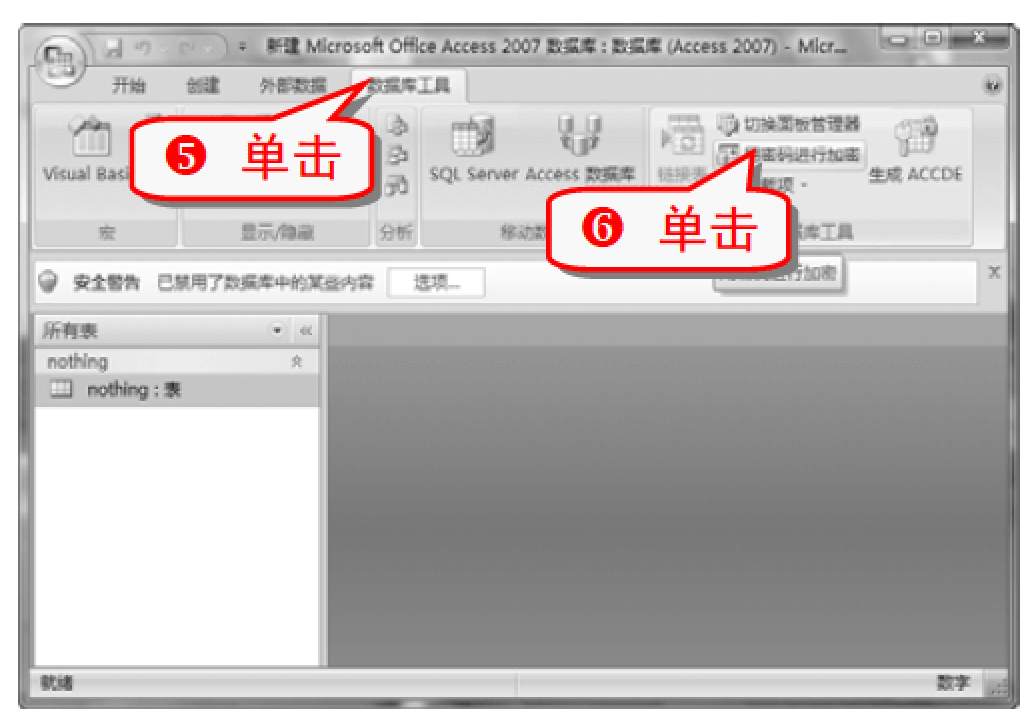
技巧72　为 Access 2007 文档设置密码

Access 2007 里如果存放着重要的表格，就有必要对其进行加密。

❶ 选择“Office 按钮”→“打开”命令，弹出“打开”对话框。









注　意　事　项



必须以独占方式打开 Access 文档才能进行加密。

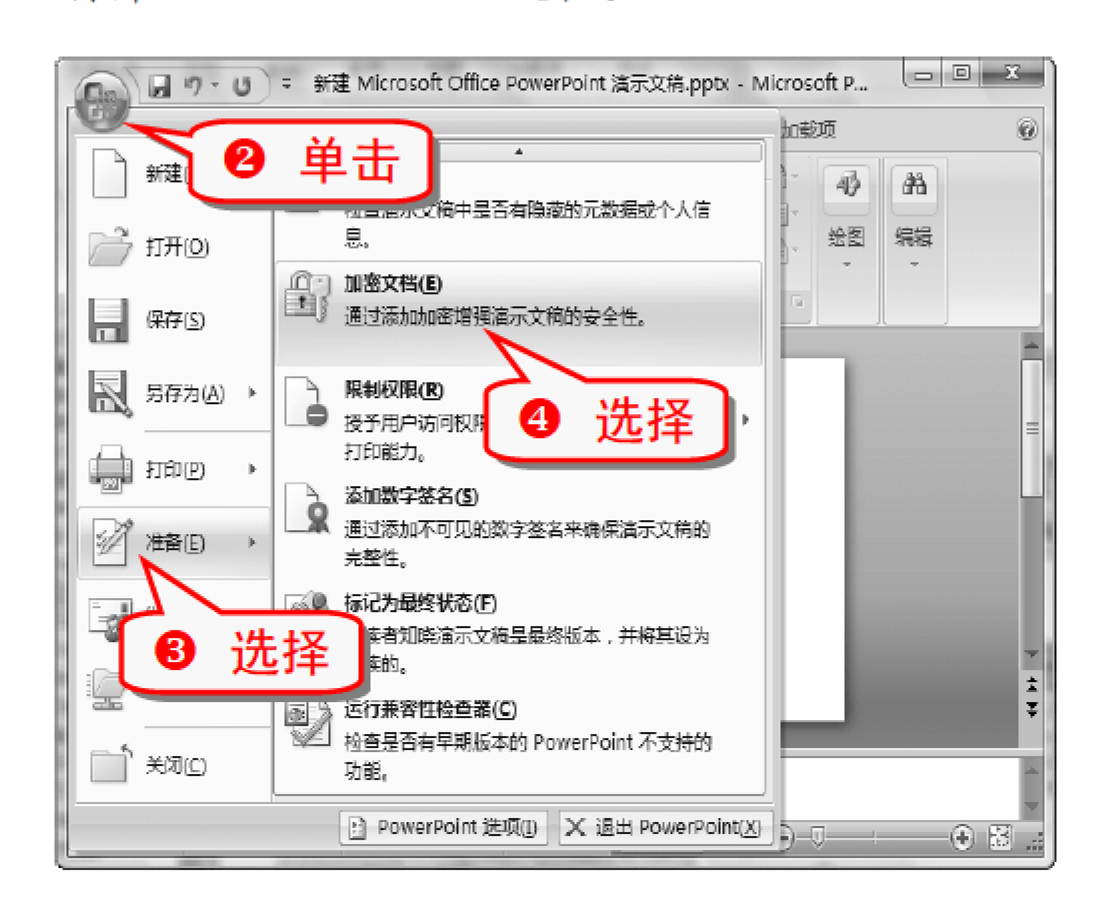
举　一　反　三

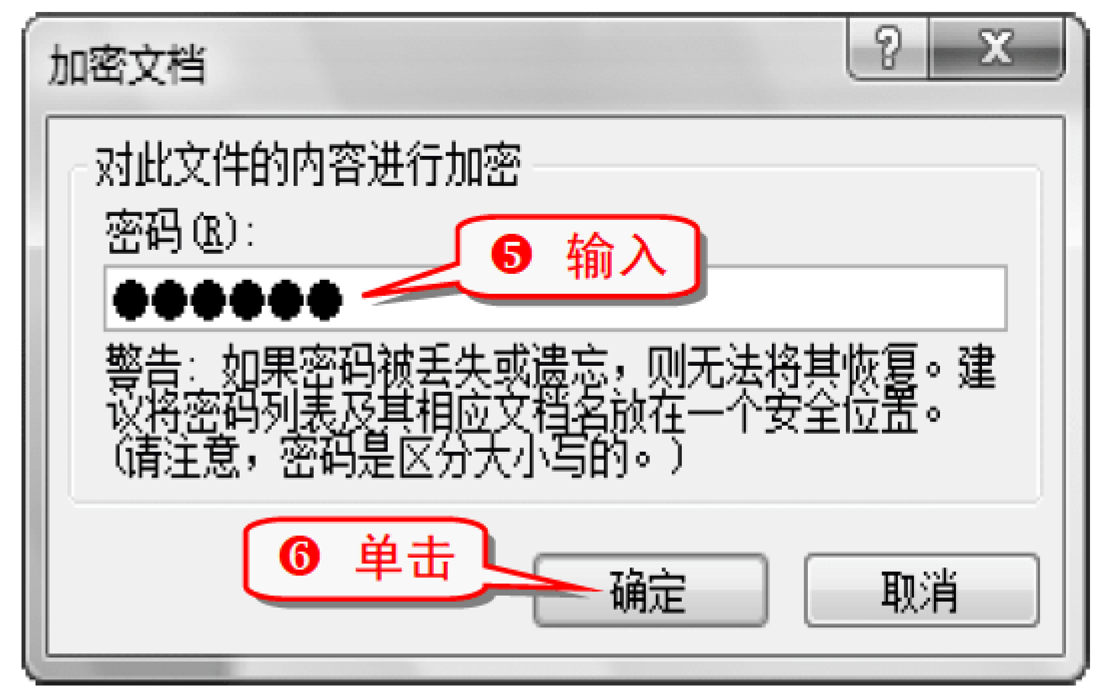
以独占方式打开 Access 文档，在“数据库工具”选项卡上的“数据库工具”组中，单击“解密数据库”按钮，在弹出的“撤销数据库密码”对话框中输入密码，然后单击“确定”按钮，就可以把密码撤销掉。

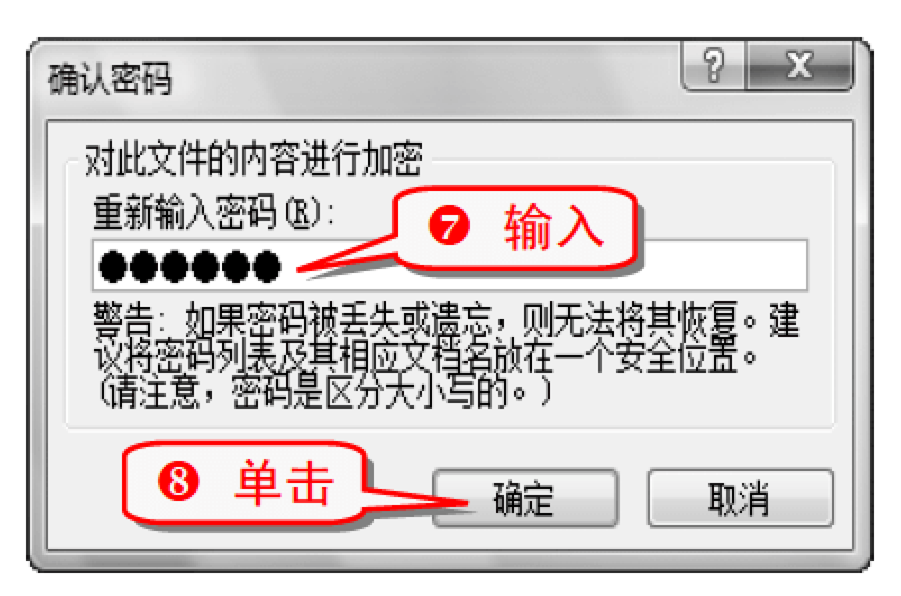
技巧73　为 PowerPoint 2007 文档设置密码

对 PowerPoint 2007 文档进行加密的步骤如下。

❶ 打开 PowerPoint 2007 文档。







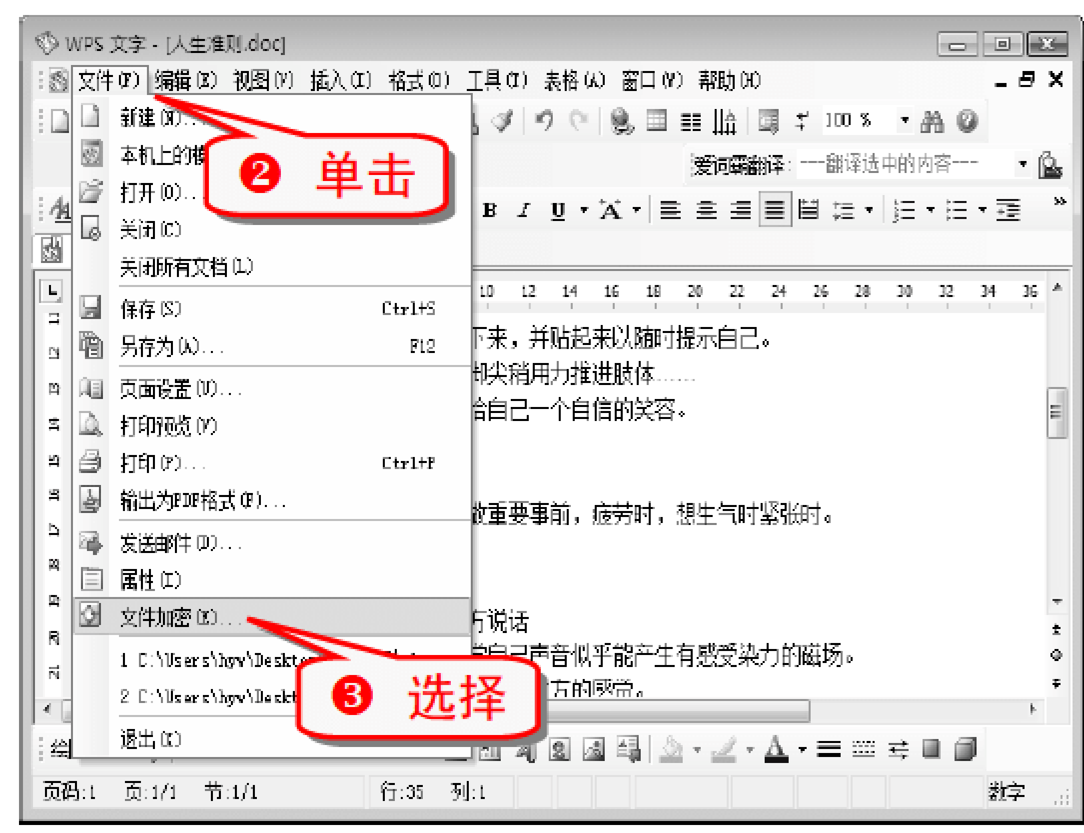
举 一 反 三

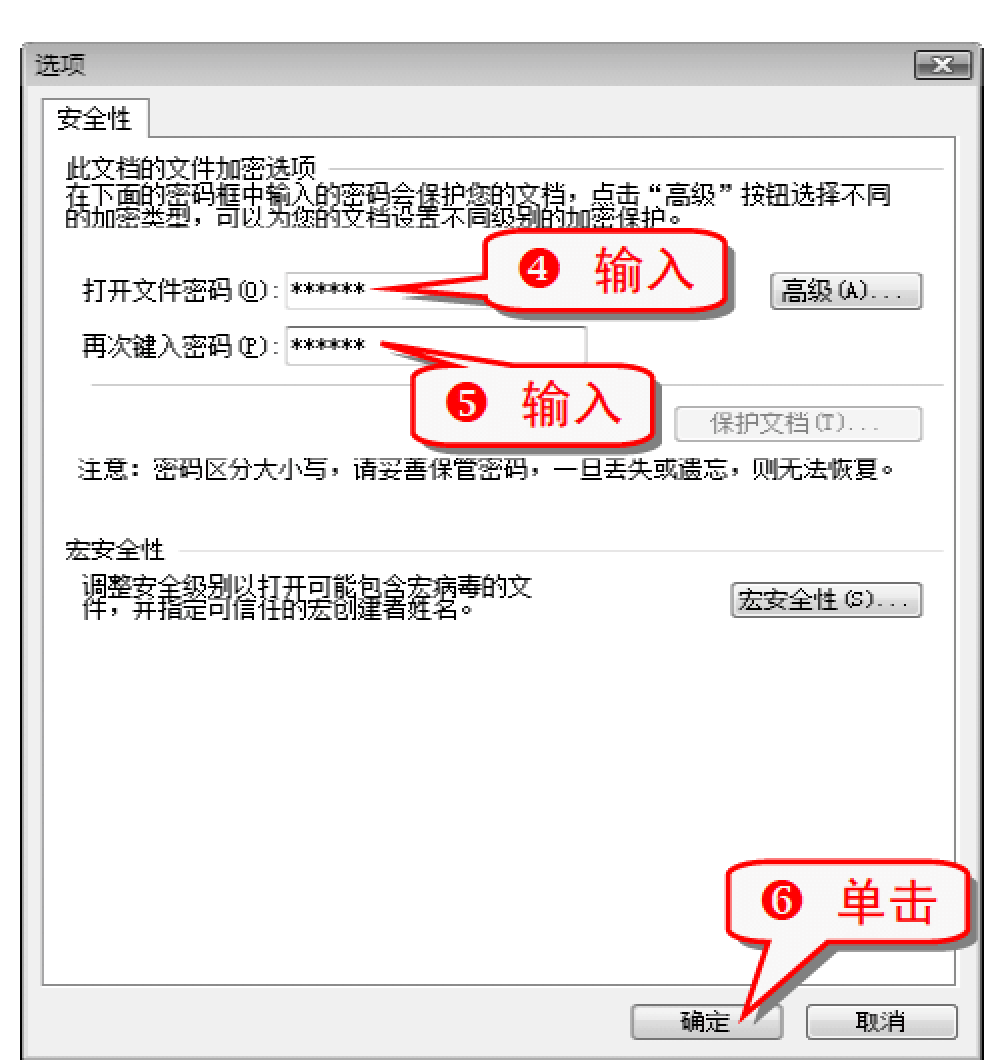
单击按钮，选择“另存为”命令，或者直接按下F12键，在弹出的“另存为”对话框中选择“工具”→“常规选项”命令，选择要删除的密码，然后按下Delete键，单击“确定”按钮，就可以把PowerPoint 2007文档的密码删除掉。

技巧74 为 WPS 2007 文档设置密码

对WPS 2007文档进行加密的步骤如下。

❶ 打开WPS 2007文档。

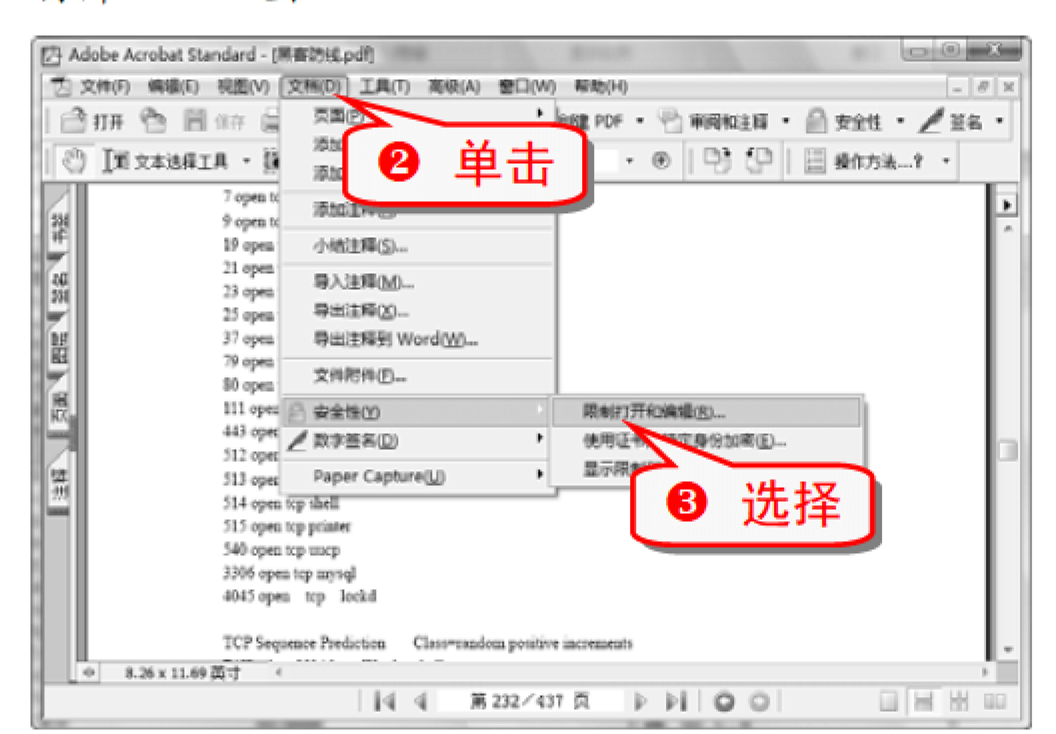




技巧75 为 PDF 文档设置密码

对PDF文档进行加密的步骤如下。

❶ 打开PDF文档。





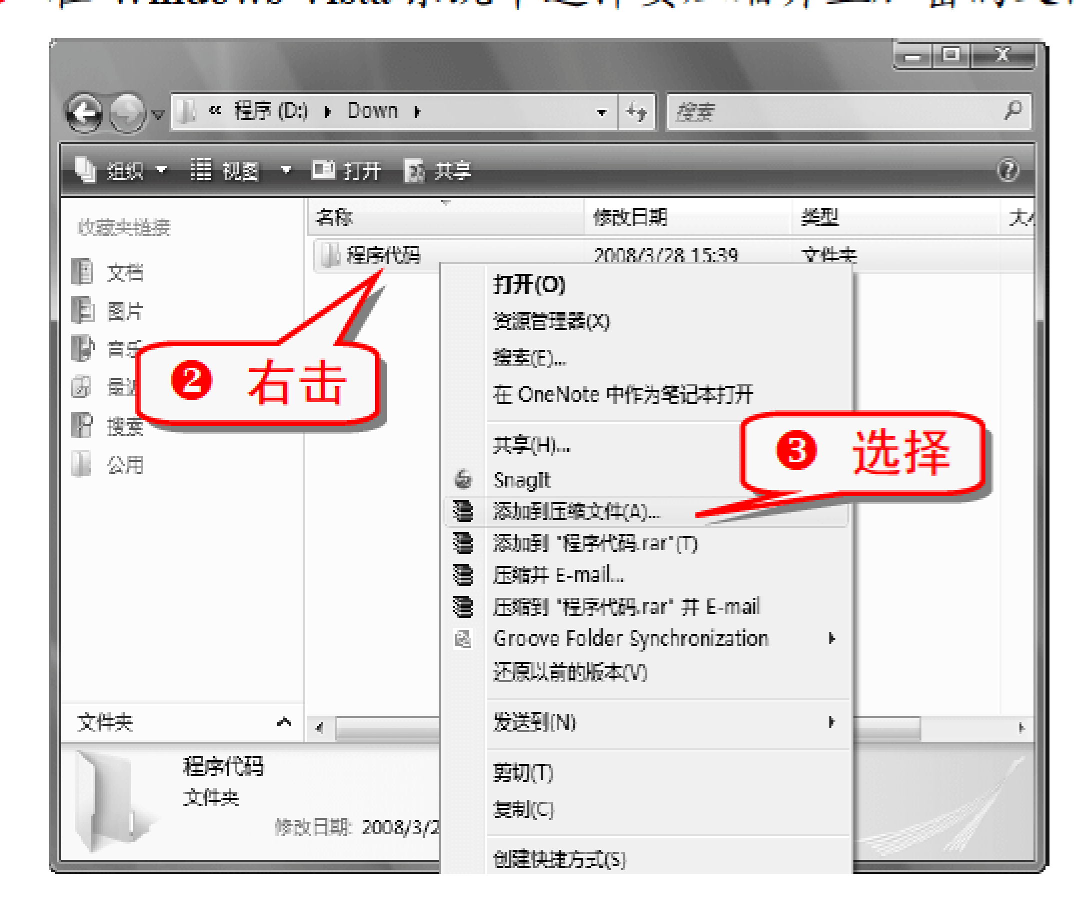




技巧76　为 WinRAR 压缩文件添加密码

网络上很多下载的压缩文件解压的时候需要输入密码，只要通过简单的几步就能做到给 WinRAR 压缩文件加密。

❶ 在 Windows Vista 系统中选择要压缩并且加密的文件。





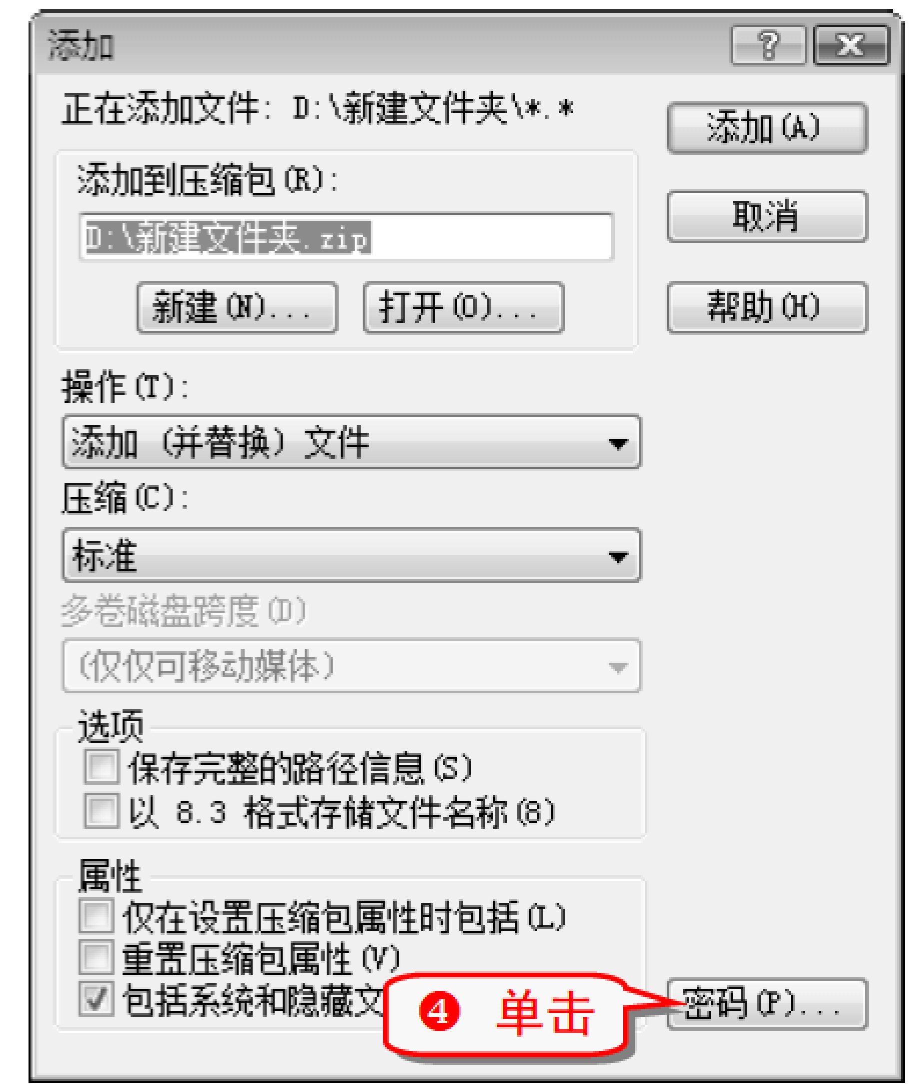


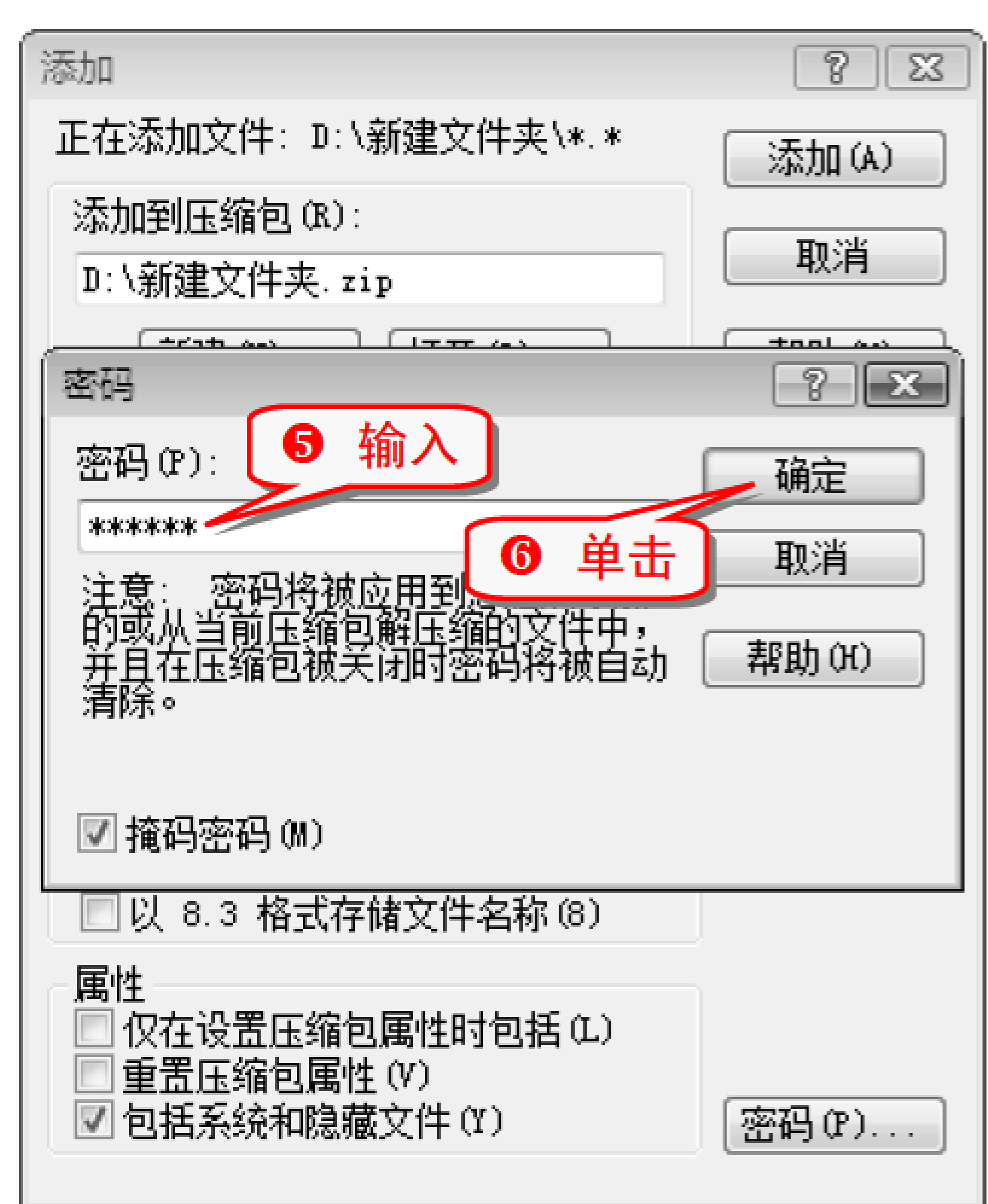
技巧77　为 ZIP 压缩文件添加密码

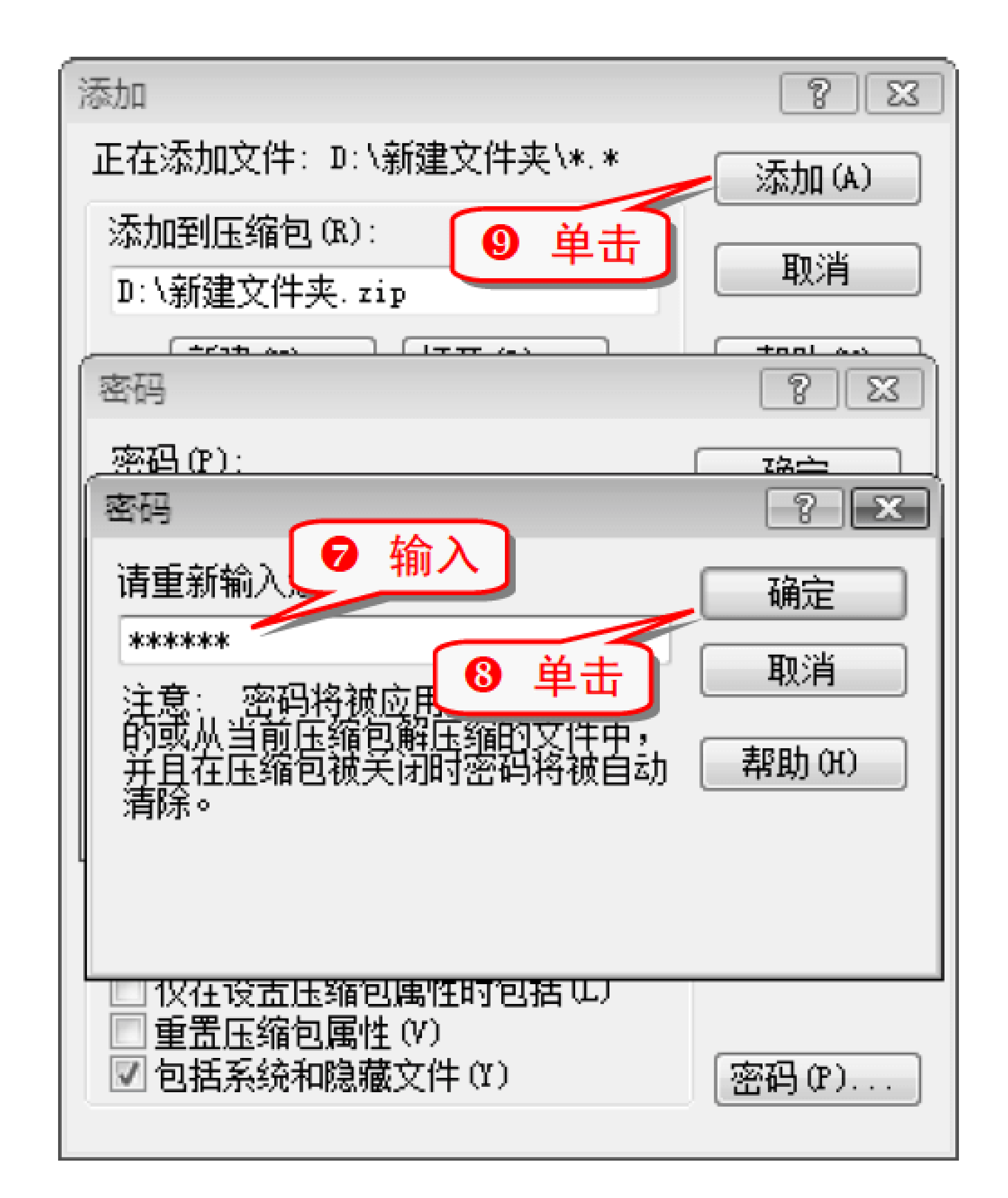
给 ZIP 压缩软件加密与给 WinRAR 压缩软件加密方法相似。

❶ 在 Windows Vista 系统中选择要压缩并且加密的文件。









技巧78　用万能加密器给文件加密

用户可以利用万能加密器给重要文件加密。

❶ 打开万能加密器。







知 识 补 充

可以通过万能加密器的解密功能为已加密文件解密，步骤类似。

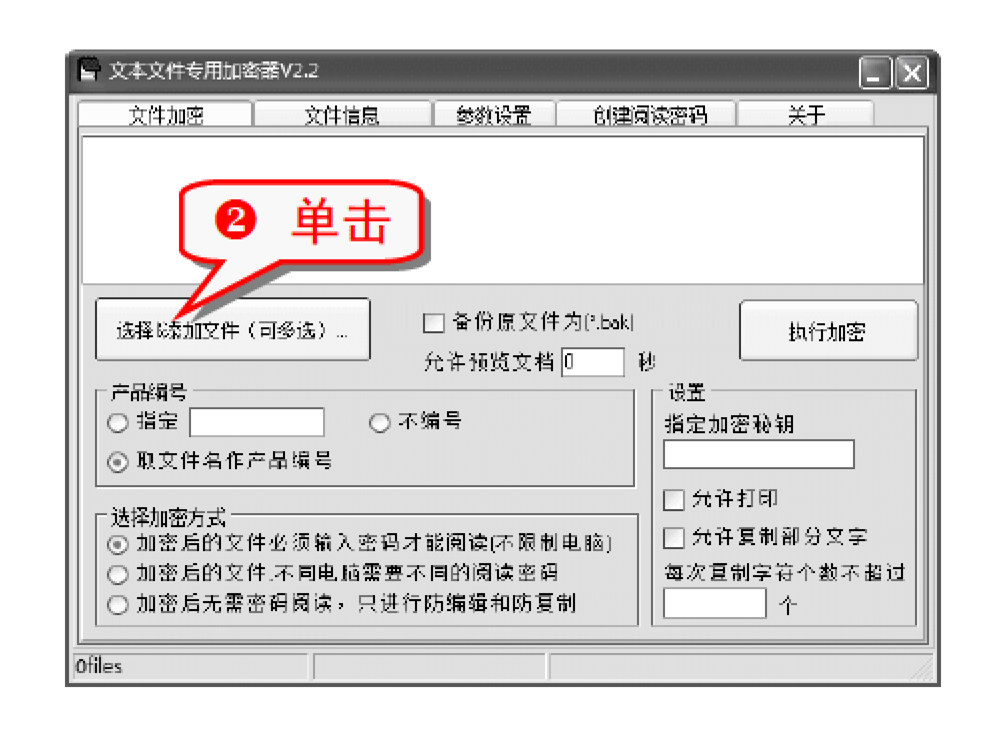
专 家 坐 堂

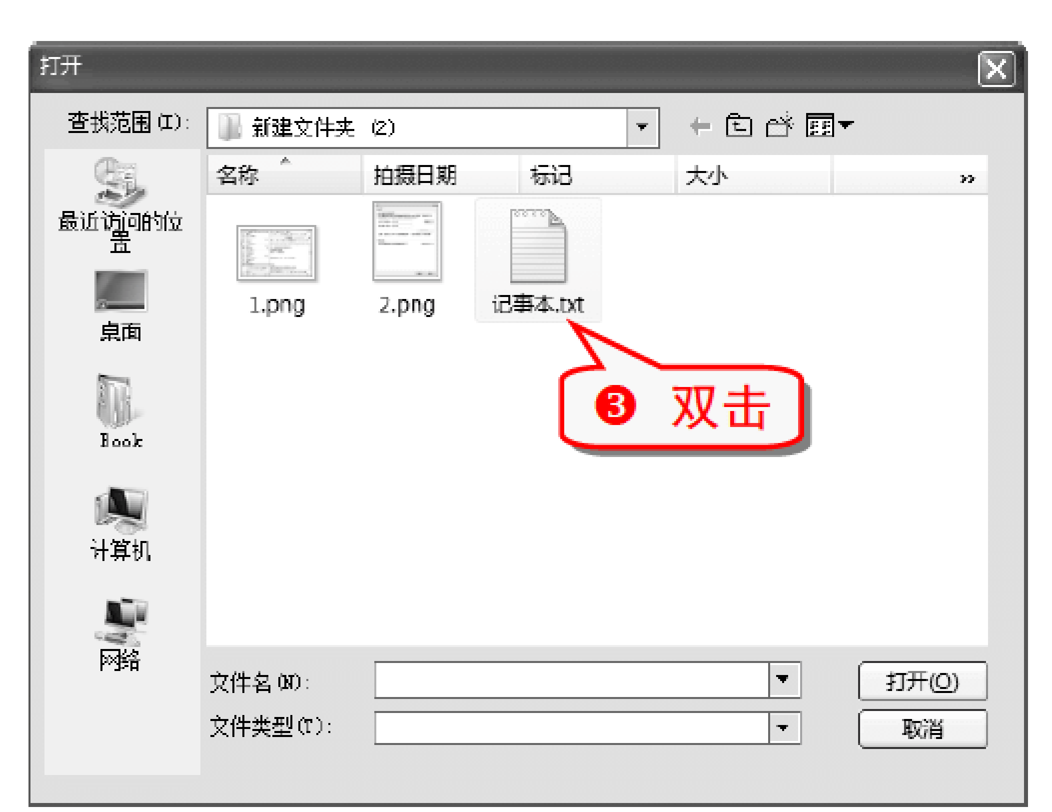
用万能加密器进行加密的时候可以利用其“产生随机密码”的功能，产生一个安全性比较强的随机密码。

技巧79　用文本加密器给文本文件加密

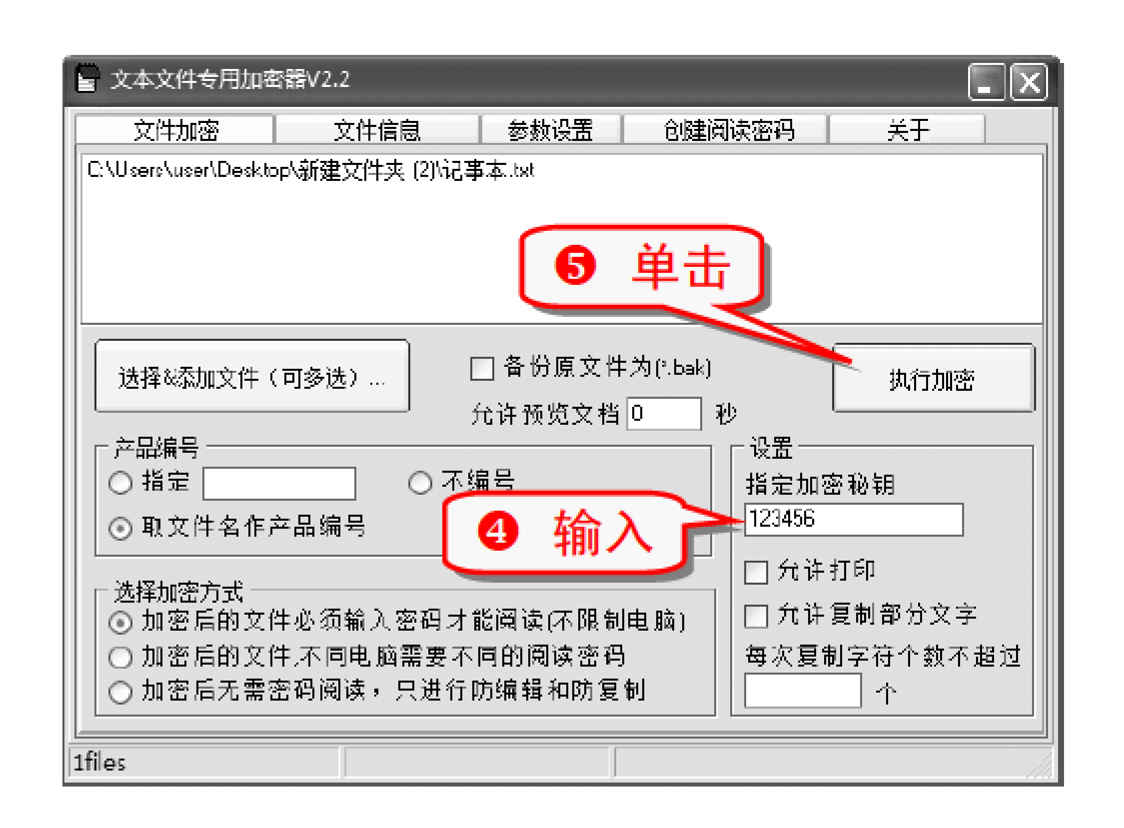
这里介绍一个专用的文本加密工具“文本文件专用加密器 V2.2”。

❶ 运行文本文件专用加密器 V2.2。





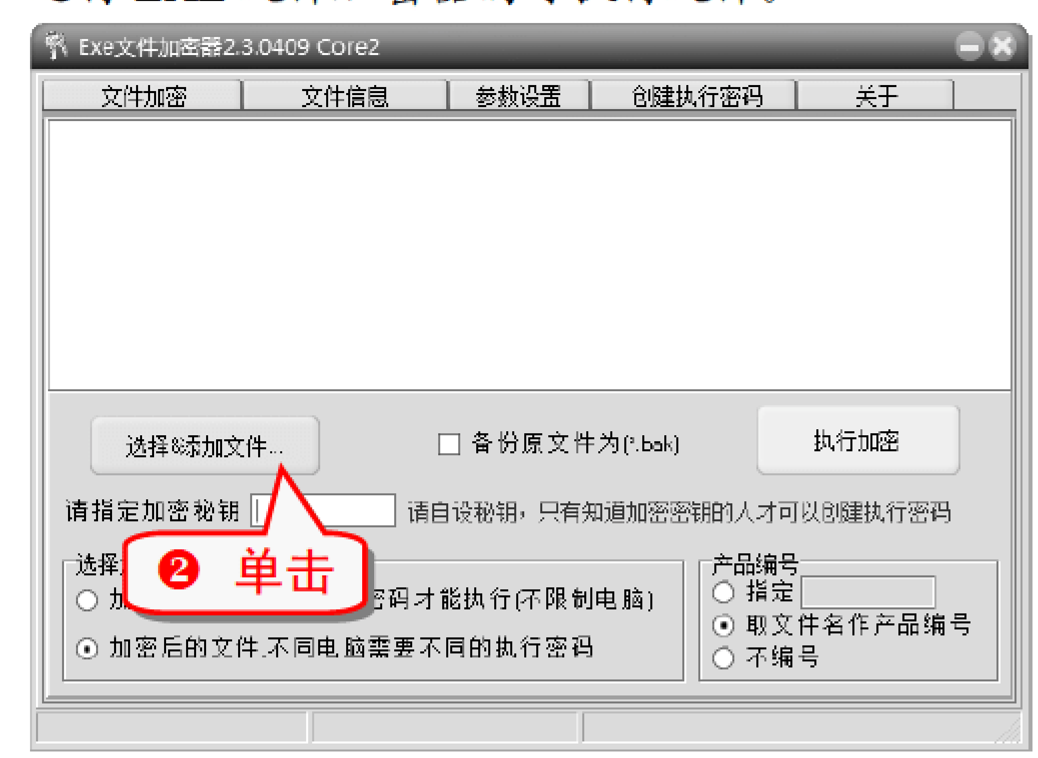


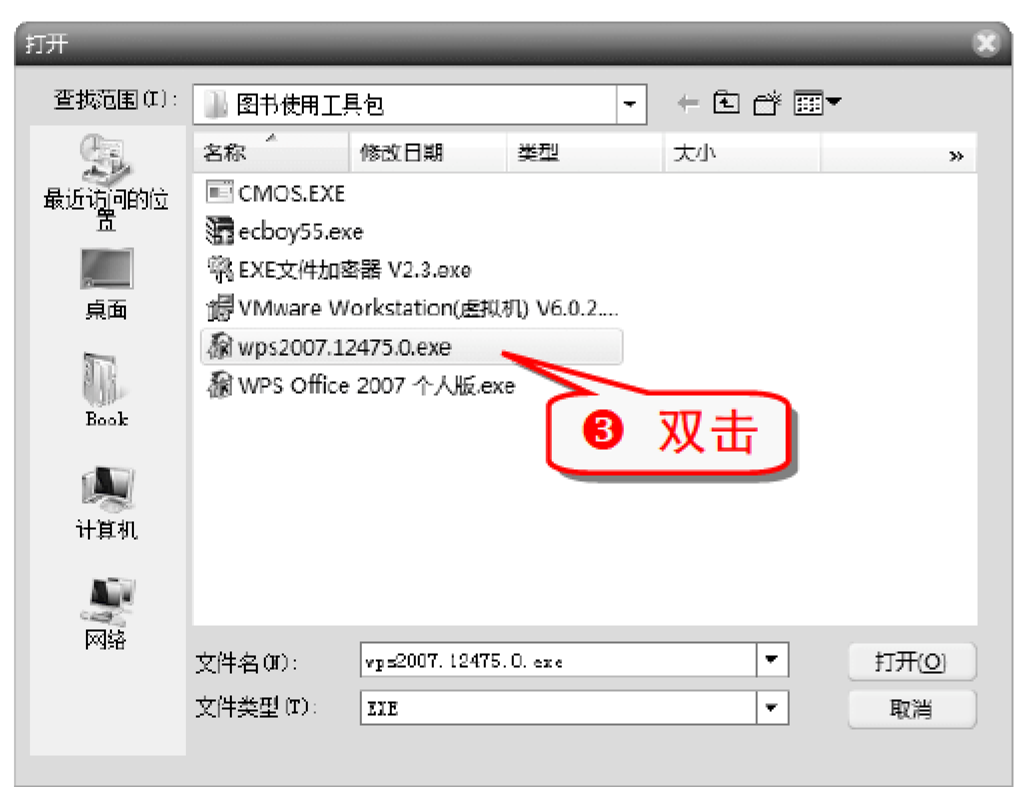


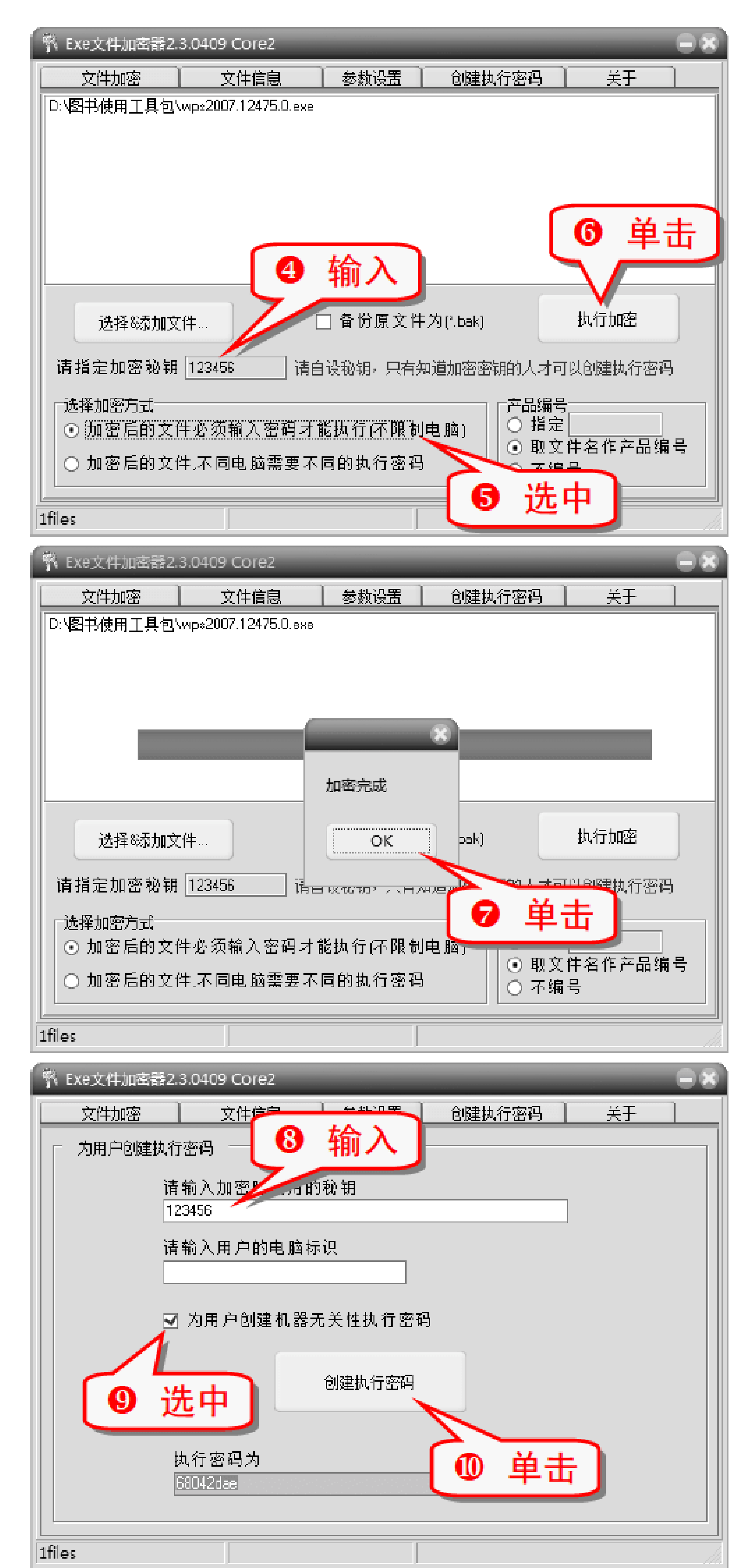
技巧80　用 EXE 文件加密器给文件加密

给电脑上的 EXE 文件加上密码，他人就无法使用 EXE 文件，除非输入正确的密码。EXE 文件加密器可以从网上下载。

❶ 运行 EXE 文件加密器的可执行文件。







知　识　补　充

给 EXE 文件加密后，如果要执行已经加密的 EXE 文件，必须输入执行密码。

技巧81　用 Lock My PC 锁定电脑

Lock My PC 可以从网上下载到，是一个体积小却非常好用的软件，可以快速将电脑锁定起来。

❶ 双击 Lock PC.EXE 文件，右击桌面右下角出现的图标。





❺ 右击桌面右下角的图标，在弹出的快捷菜单中选择“锁定计算机”命令，电脑进入锁定状态。



举 一 反 三

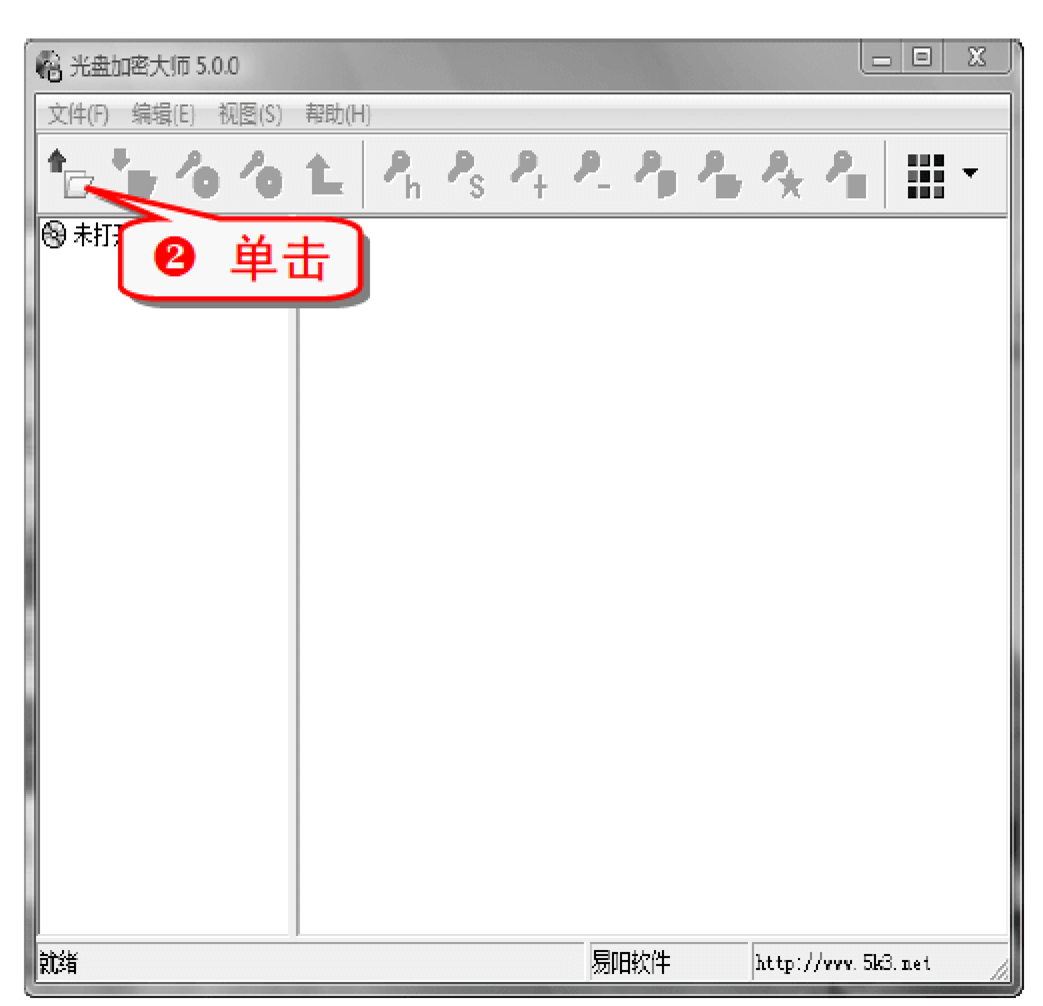
用户不仅可以手动锁定电脑，还可以通过右击，然后使用弹出的快捷菜单中的“设置”命令将电脑设置为：非法关机后锁定，启动时锁定。在这个选项中也可以为电脑的锁定屏幕选择一个喜欢的图像。

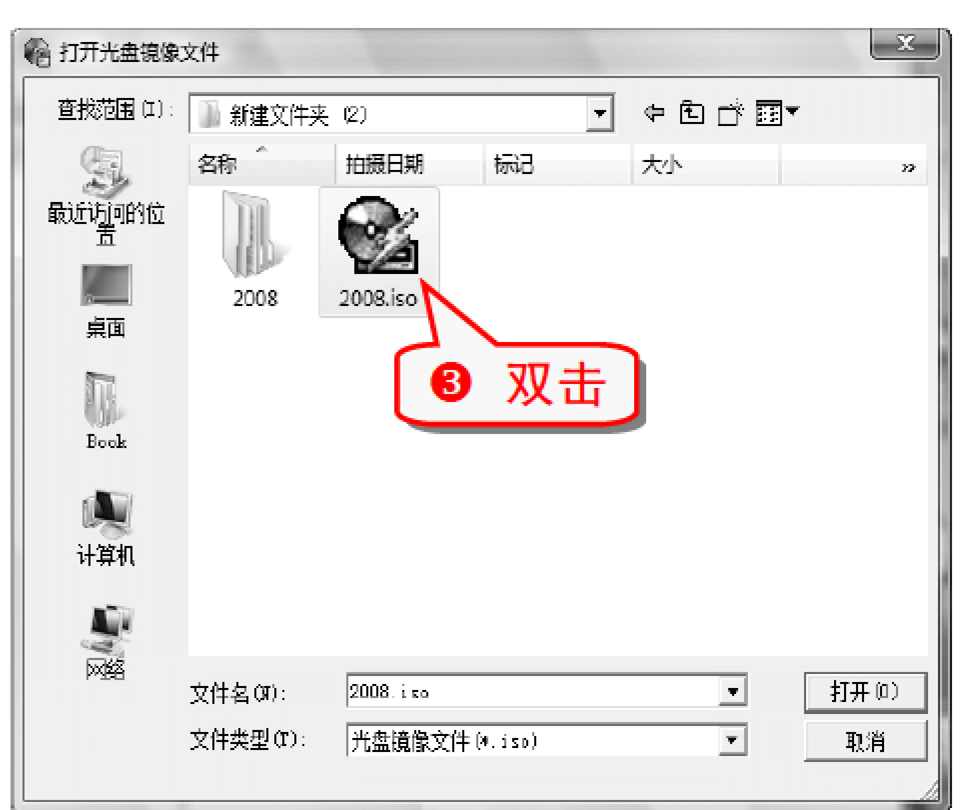
在 Windows Vista 中也提供了电脑锁定功能，只要按下 + L 组合键，不过必须是在设置了账户密码的情况下才有意义。

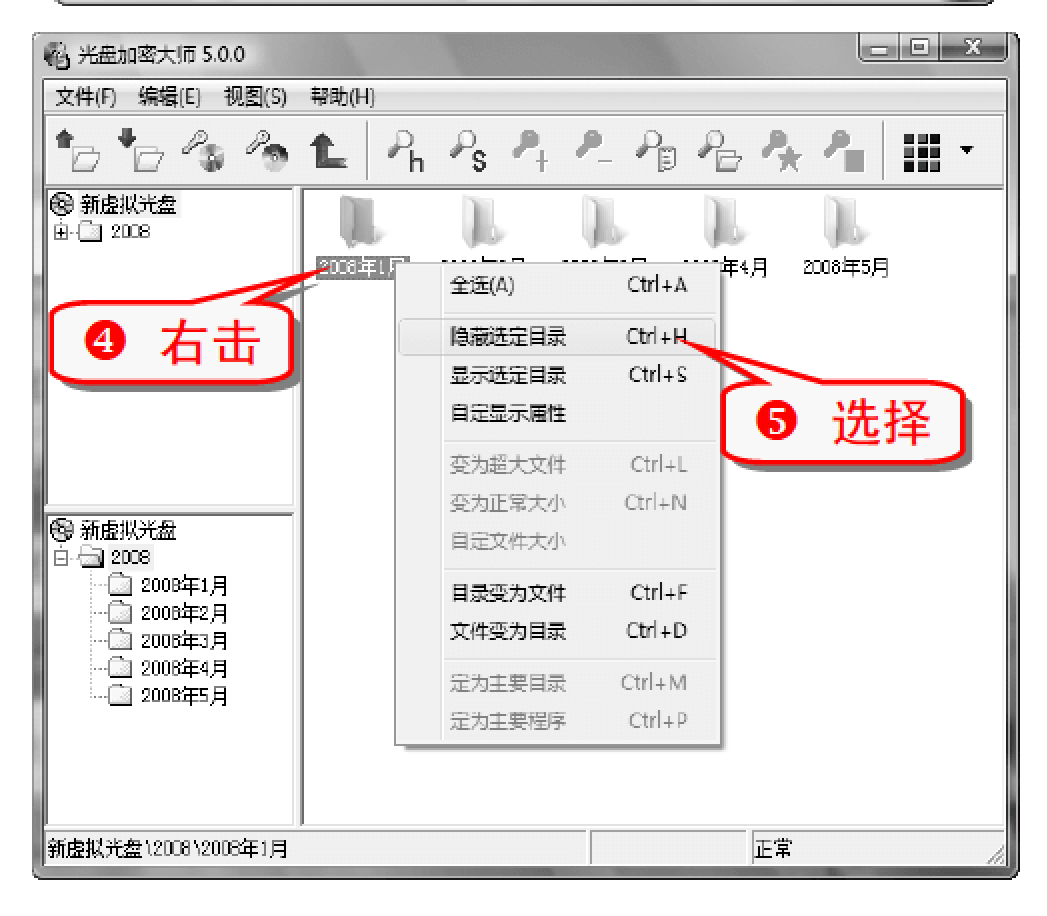
技巧82　隐藏镜像文件的目录

可以通过光盘加密大师隐藏镜像文件的目录，镜像文件被刻录成光盘时，就看不到隐藏起来的文件。

❶ 双击光盘加密大师的可执行文件，打开光盘加密大师程序主界面。





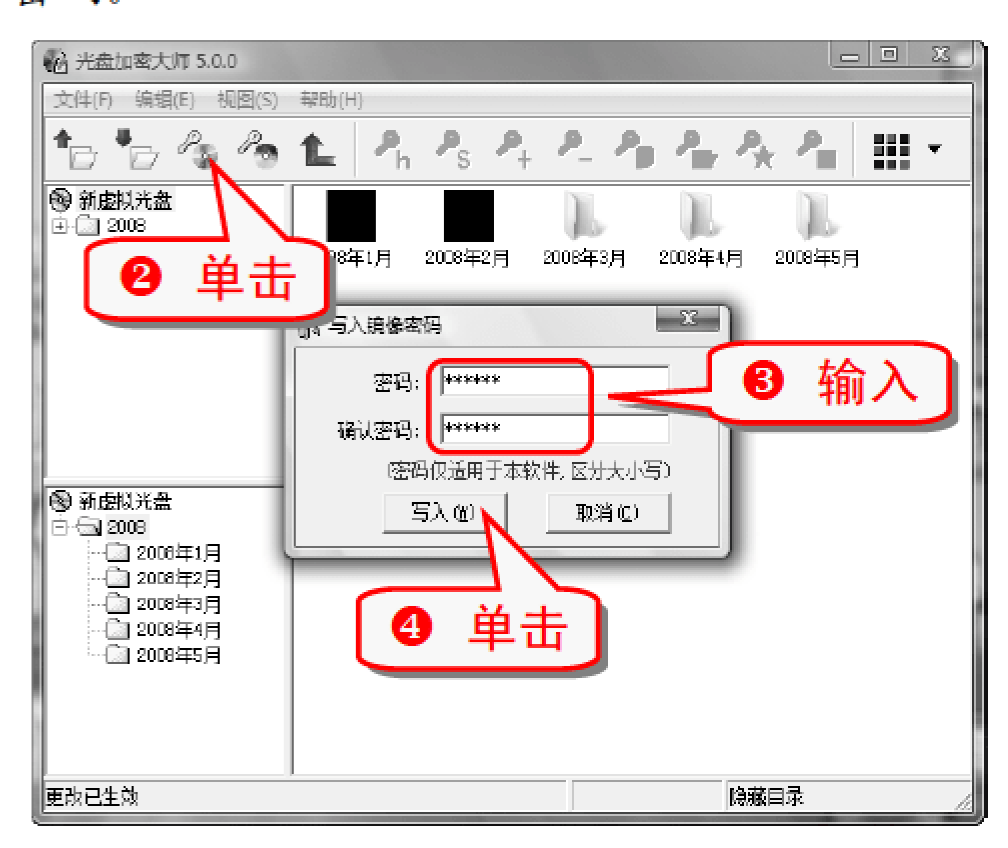


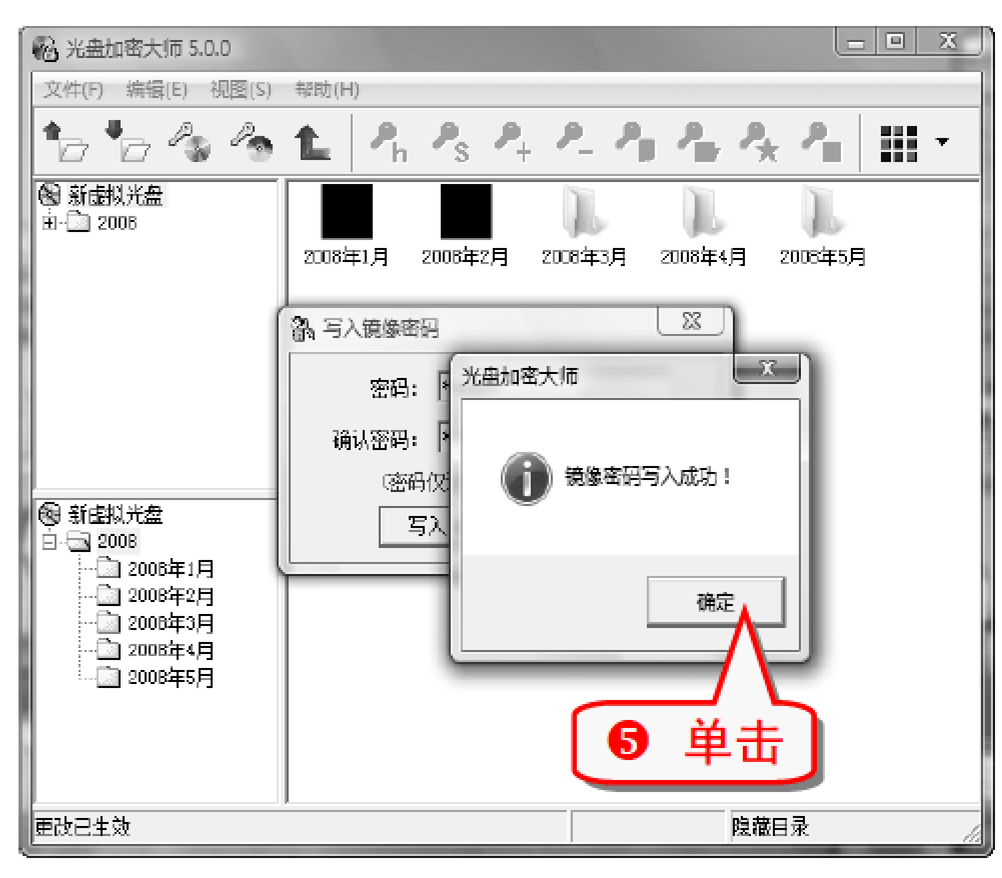


技巧83　为镜像文件设置镜像密码

可以利用光盘加密大师对镜像文件设置密码。

❶ 按照上一技巧的方法打开镜像文件，然后设置镜像密码。

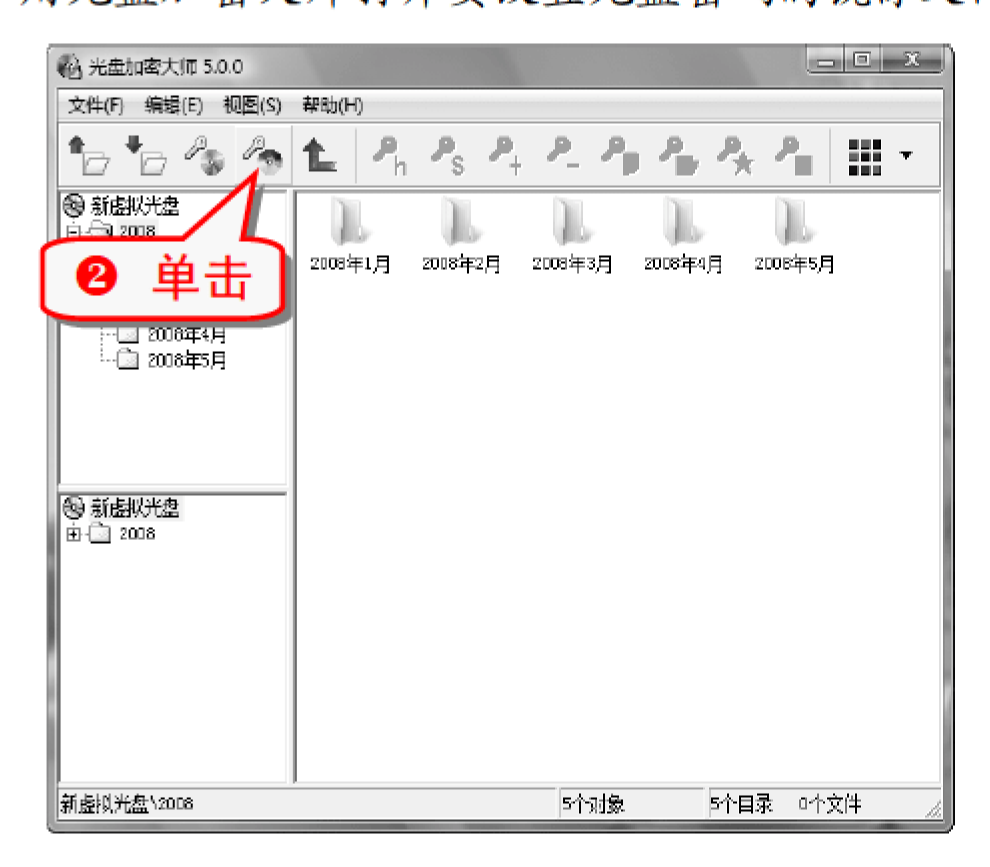


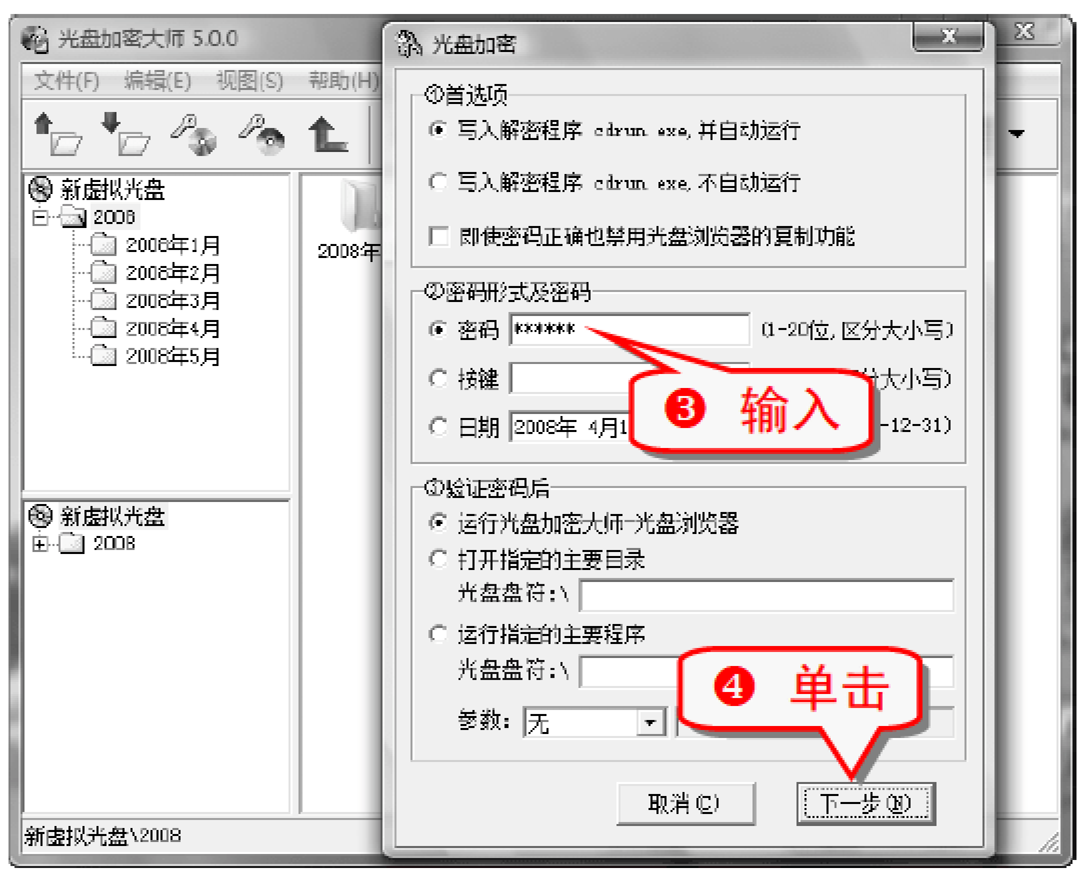


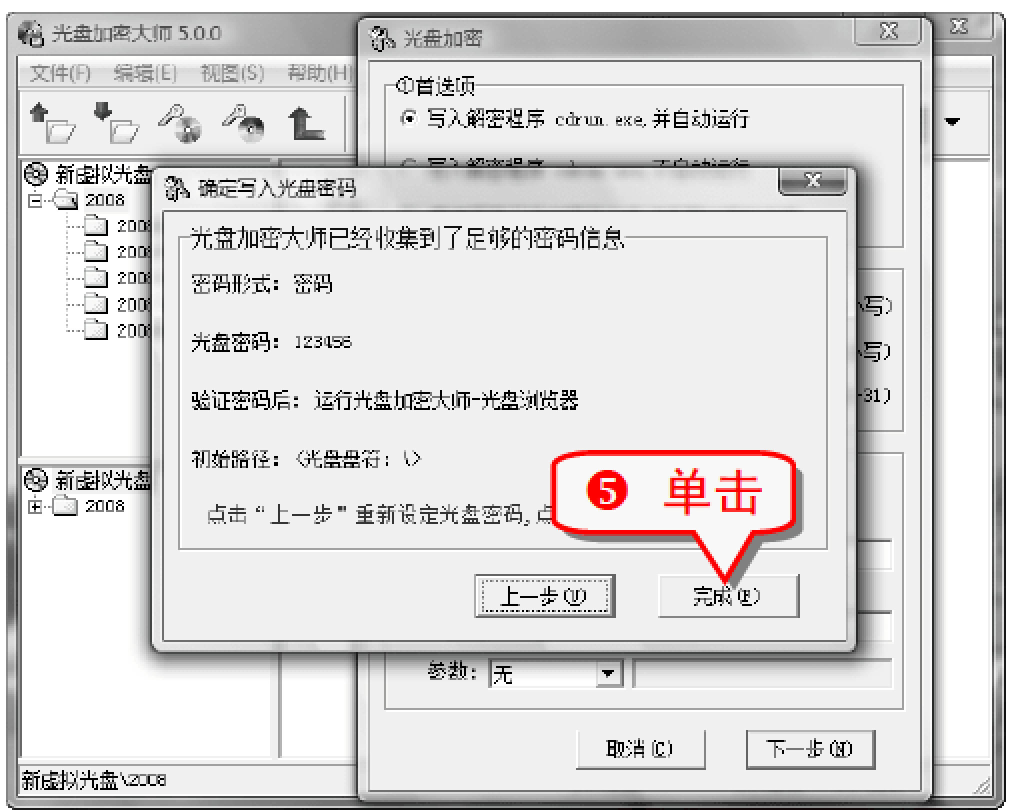
技巧84　为镜像文件设置光盘密码

可以利用光盘加密大师为镜像文件设置光盘密码。

❶ 用光盘加密大师打开要设置光盘密码的镜像文件。







知　识　补　充

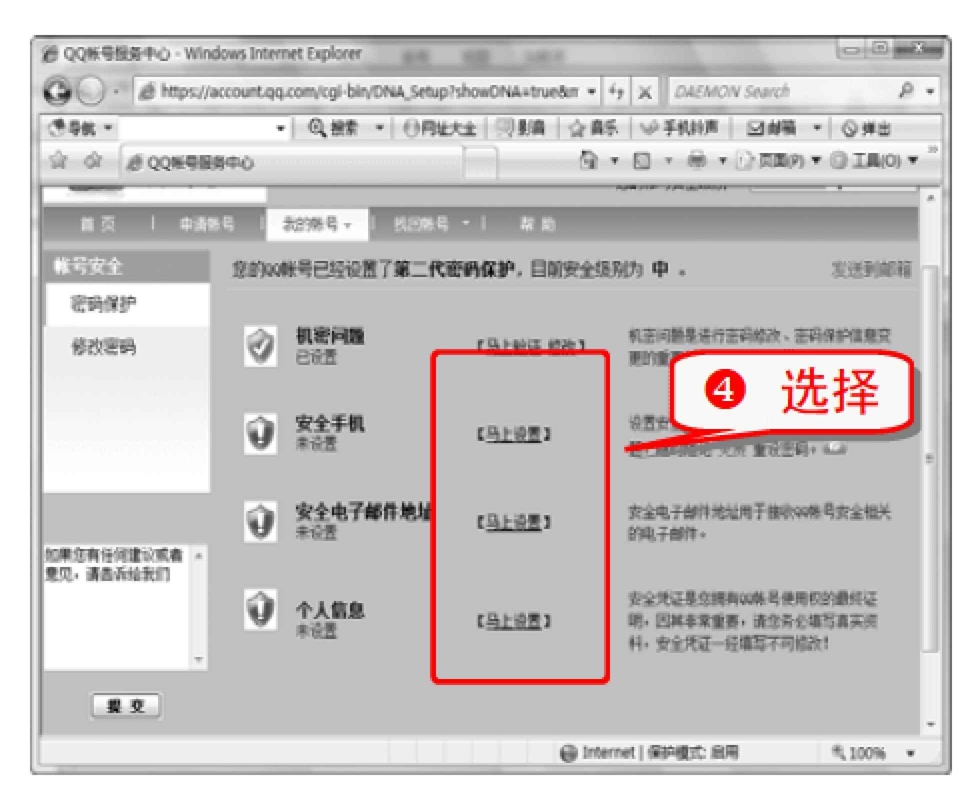
在设置镜像光盘密码的时候，除了选择密码形式还可以选择按键形式和日期形式。

技巧85　为 QQ 申请密码保护

给 QQ 申请密码保护，可以防止 QQ 被盗。

❶ 登录 QQ 2008，选择 QQ 面板上的“系统菜单”→“安全中心”→“申请密码保护”命令。

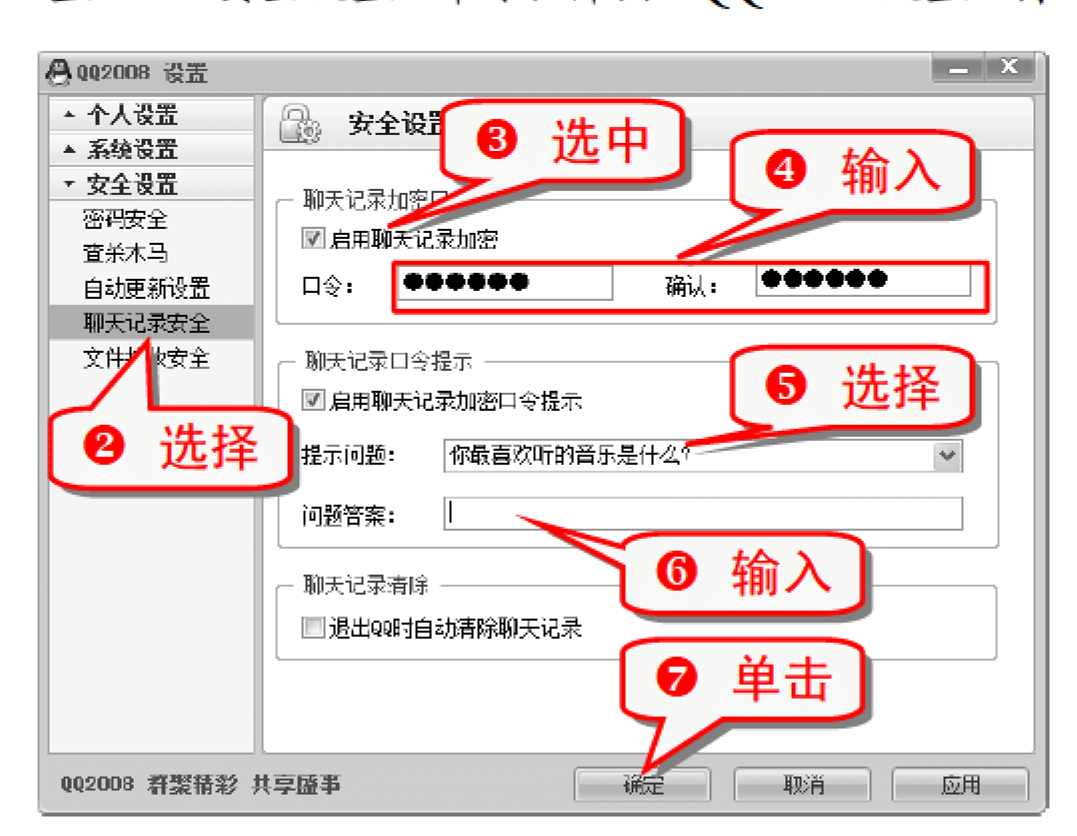




技巧86 为 QQ 聊天记录加密

有时候不愿意删除和好友的聊天记录，但是又怕被别人看到，可以为聊天记录加一个密码。

❶ 登录 QQ 2008，选择 QQ 面板上的“系统菜单”→“设置”→“安全设置”命令，弹出“QQ 2008 设置”窗口。



技巧87 为 QQ 空间加密

没有加密的 QQ 空间是对所有人都开放的，想保护自己的隐私，可以为 QQ 空间加密。

❶ 进入自己的 QQ 个人空间。





进入“开心”的 QQ 空间时，必须输入“密码问题”的答案。



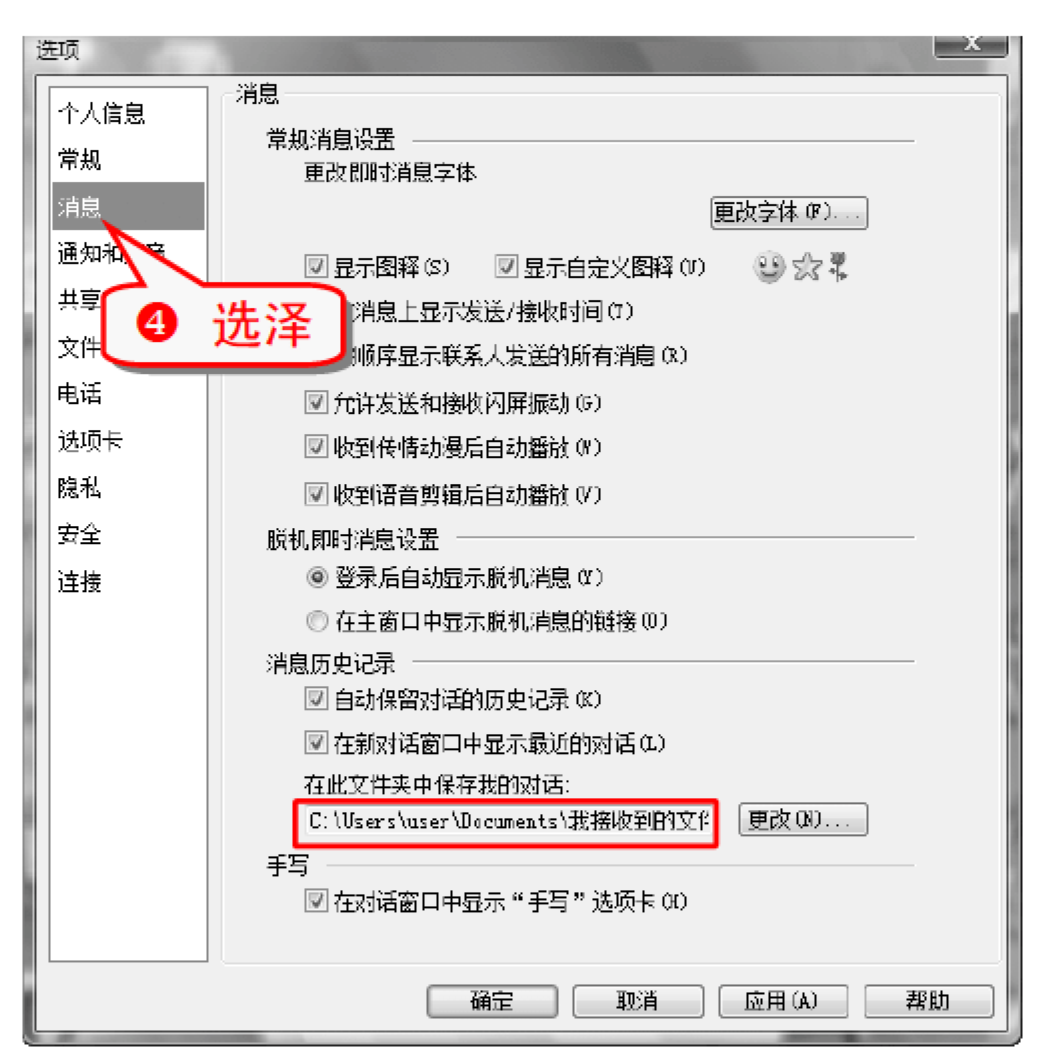
技巧88 为 MSN 聊天记录加密

可以利用 Windows Vista 加密文件系统为 MSN 聊天记录加密。

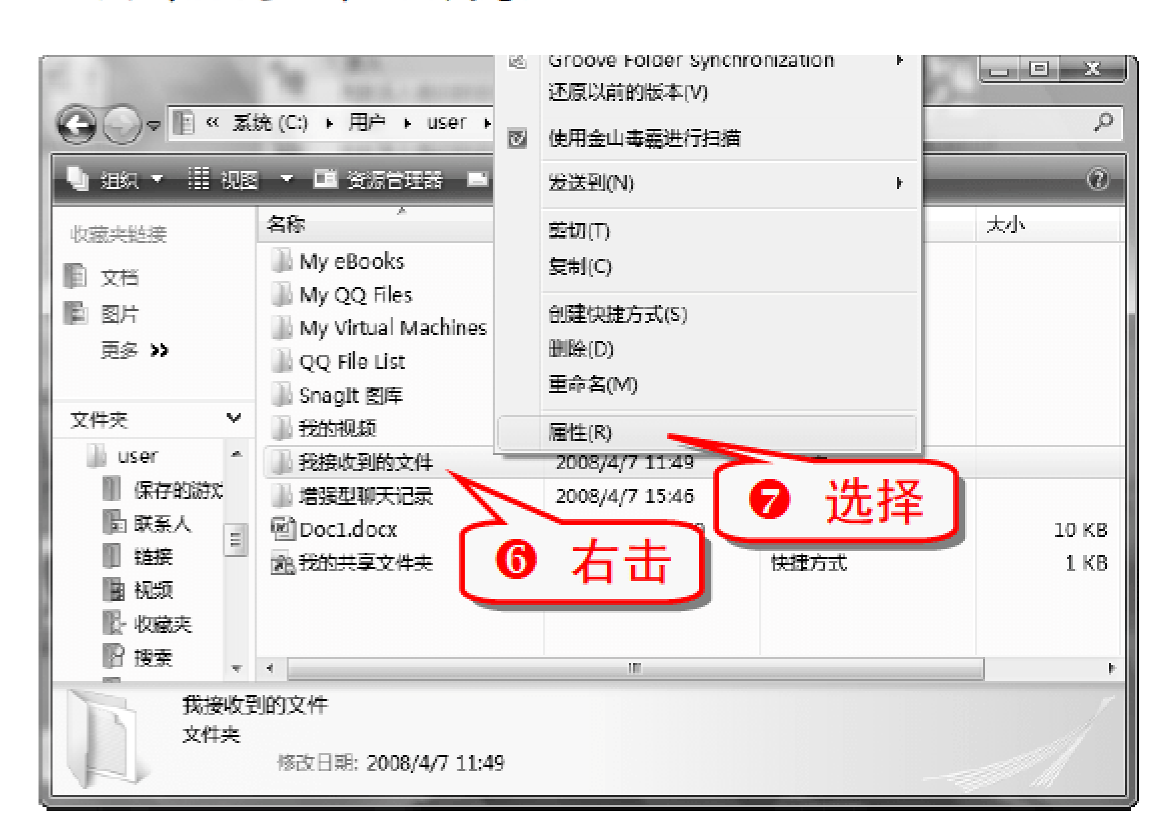
❶ 登录 MSN。

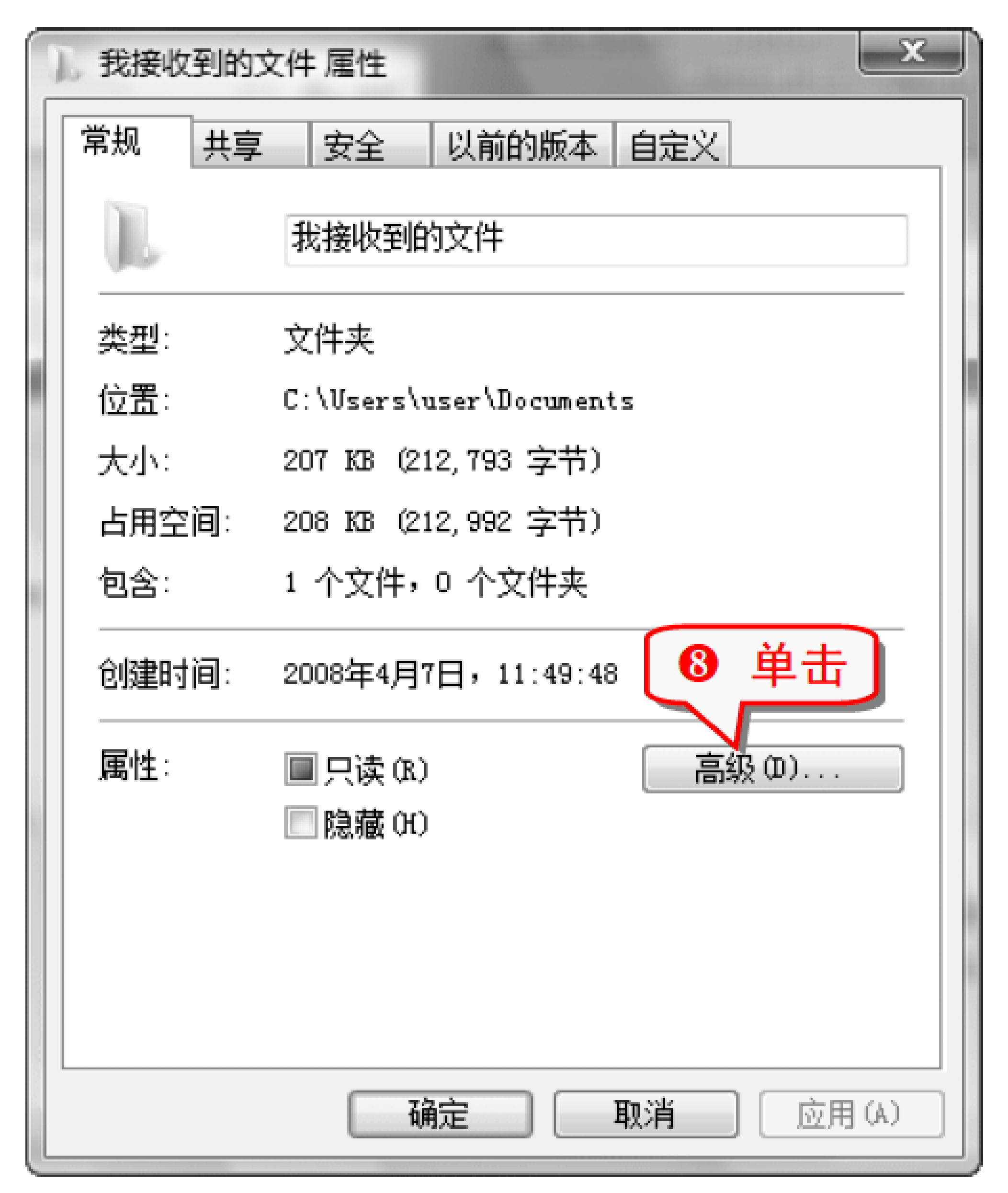


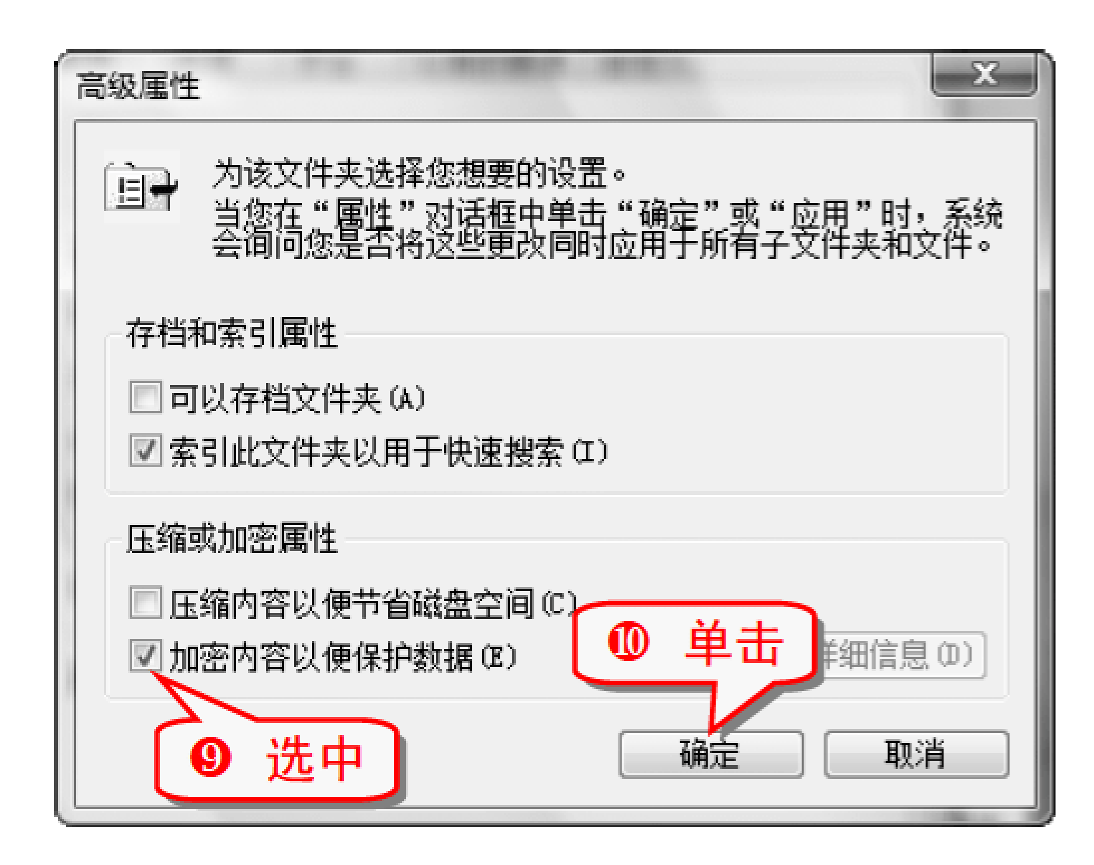




❺ 找到历史记录文件夹。



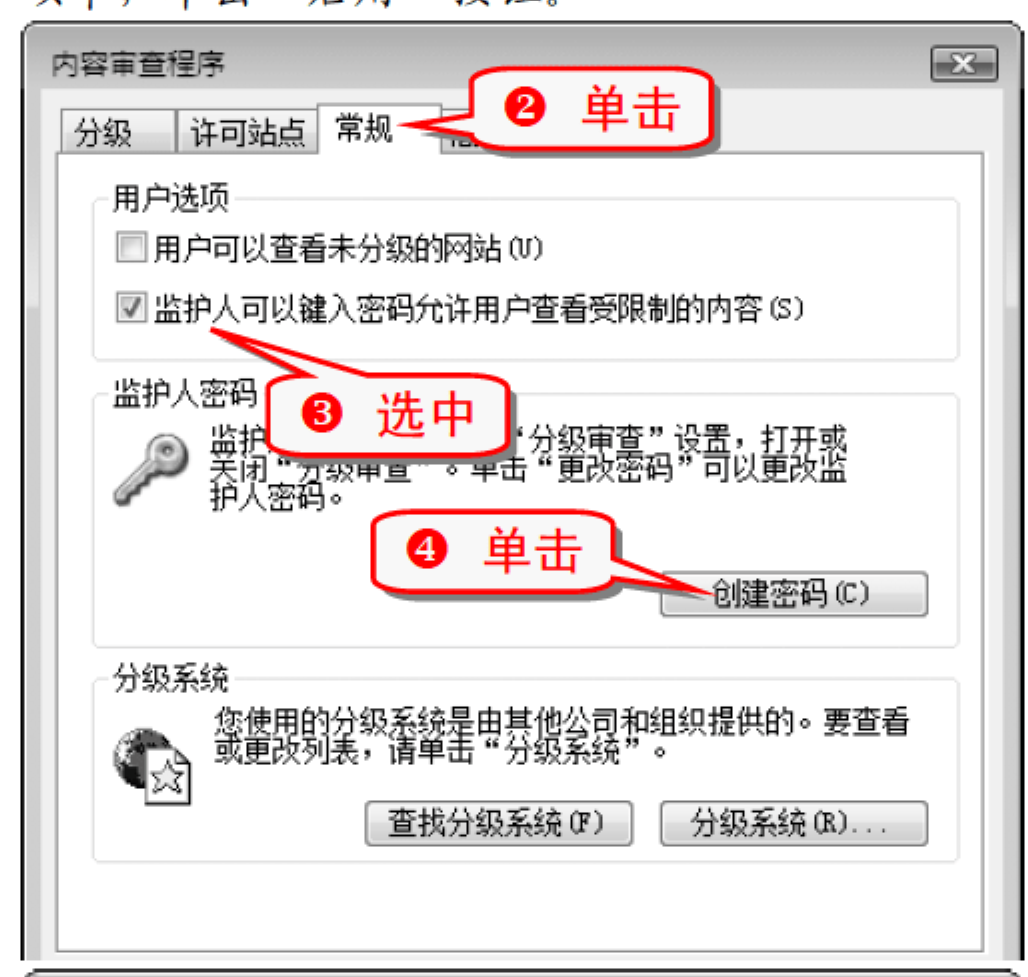


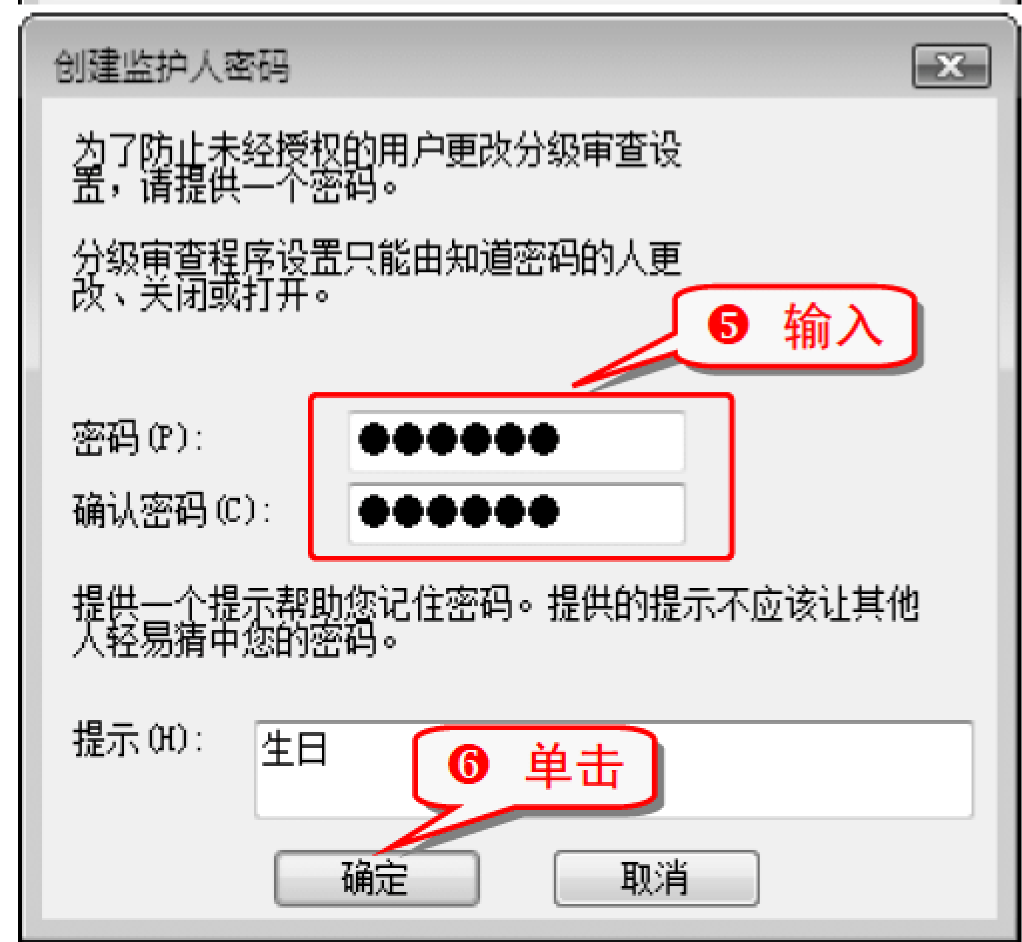


技巧89　为 IE 设置内容审查密码

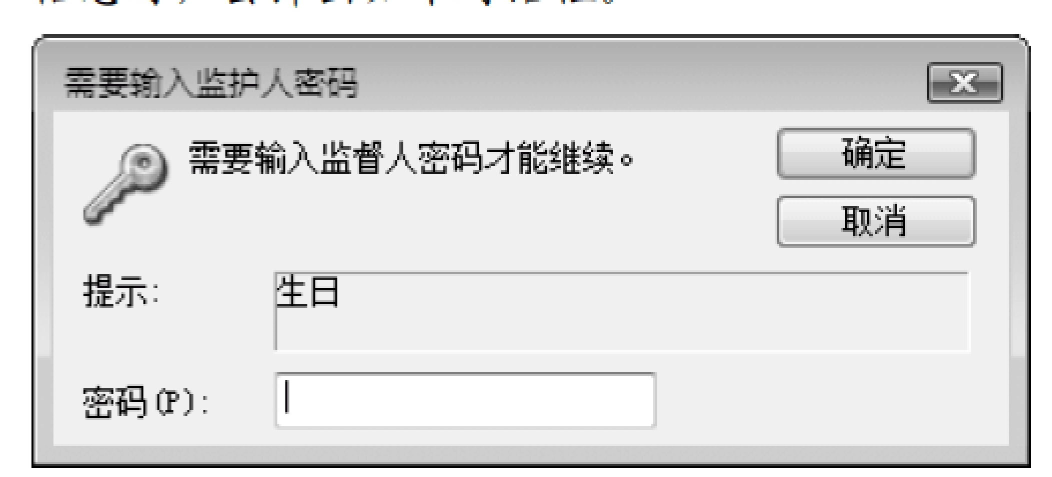
现在很多的网页包含了不良信息，为 IE 设置内容审查密码，可以过滤掉那些不良网页。

❶ 打开 IE 浏览器，选择"工具"→"Internet 选项"命令，打开"Internet 选项"对话框，切换到"内容"选项卡，单击"启用"按钮。





❼ 当要重新设置分级审查时，或者要浏览的网页有不良信息时，会弹出如下对话框。



注 意 事 项

上述设置启动了 IE 的分级审查功能，只有知道密码才能访问有不良信息的网页。

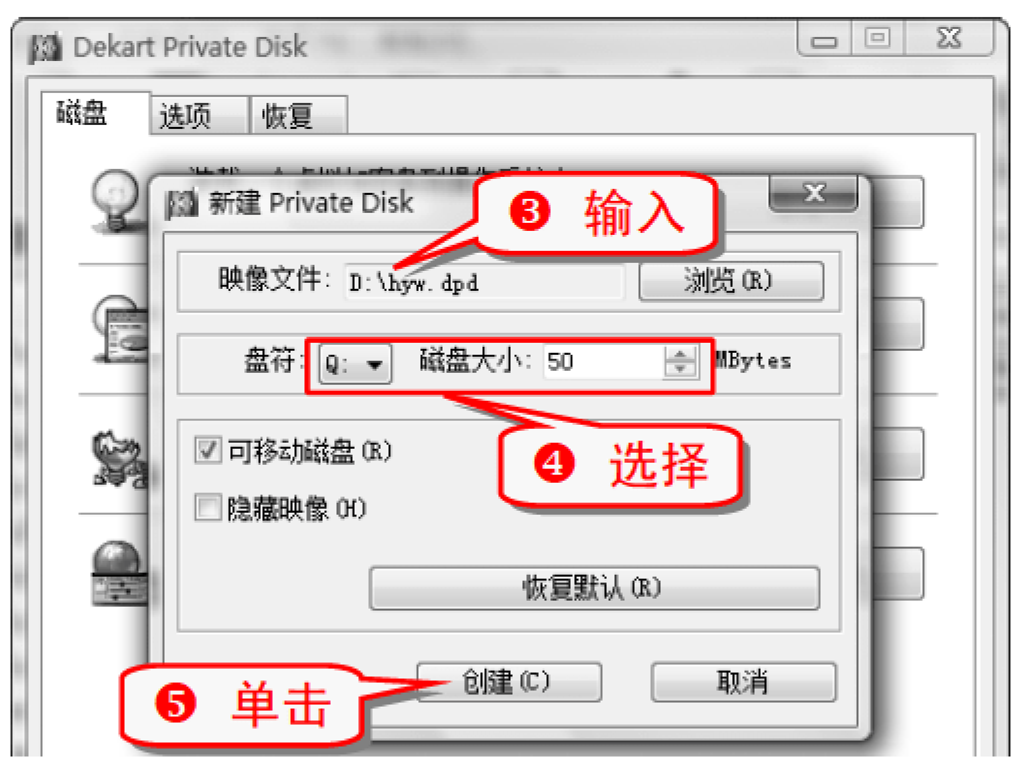
技巧90 巧用 Dekart Private Disk 保护隐私

Dekart Private Disk 软件可以建立一个加密的磁盘空间，只要将重要的文件放进去即可轻松实现加密。Dekart Private Disk 软件是一个绿色软件，不用安装。

(1) 创建虚拟加密磁盘

❶ 双击解压文件夹中的“PrvDisk.exe”文件。



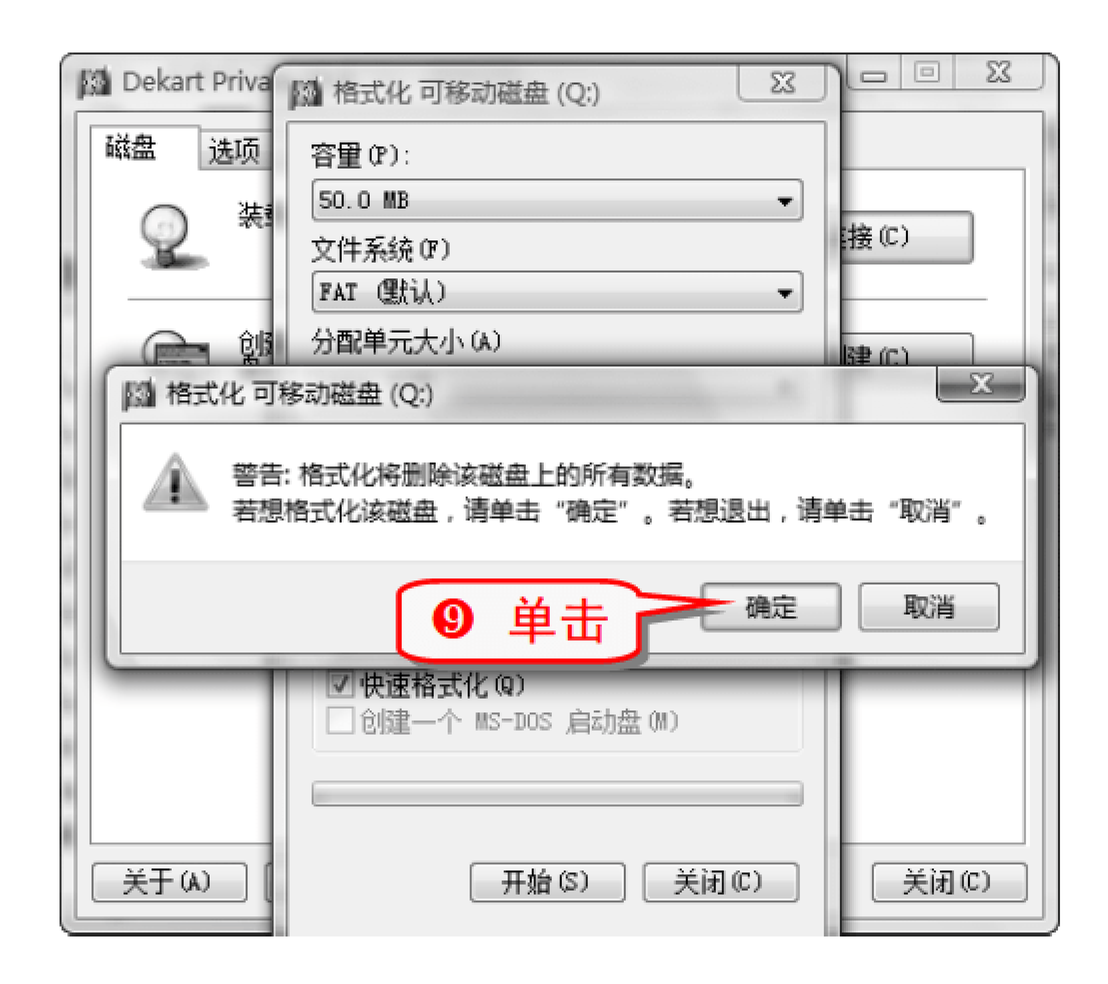


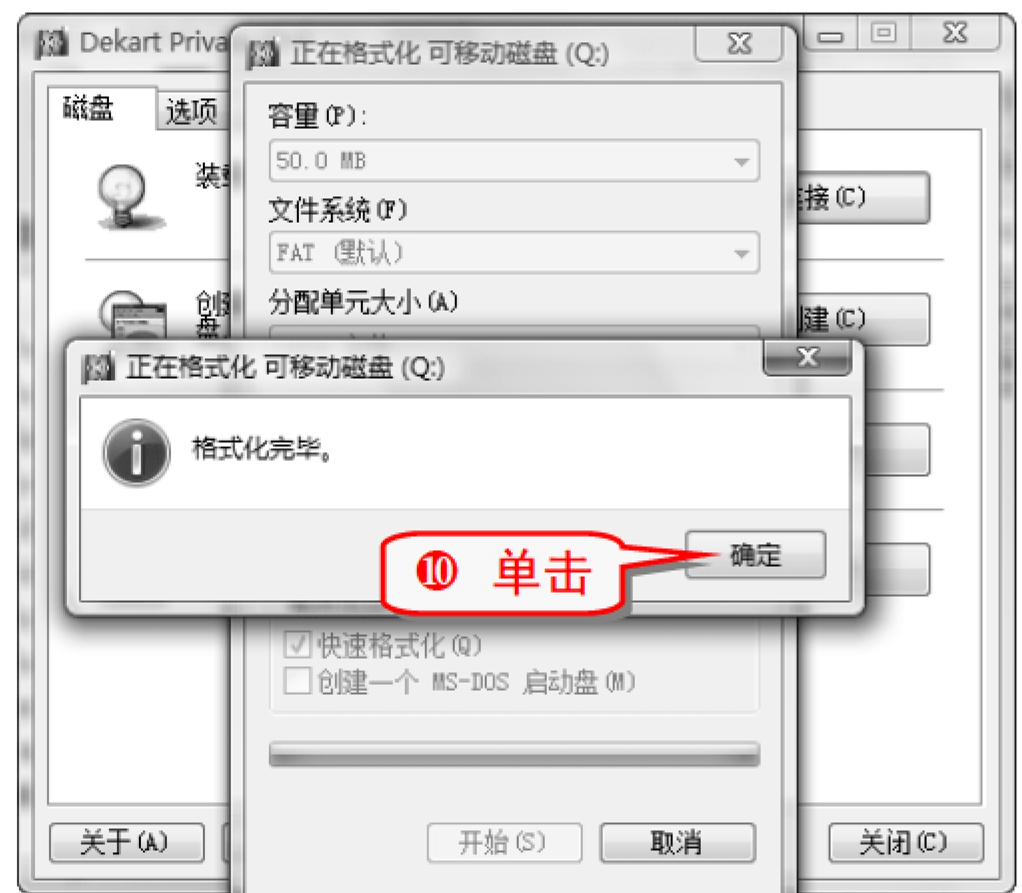


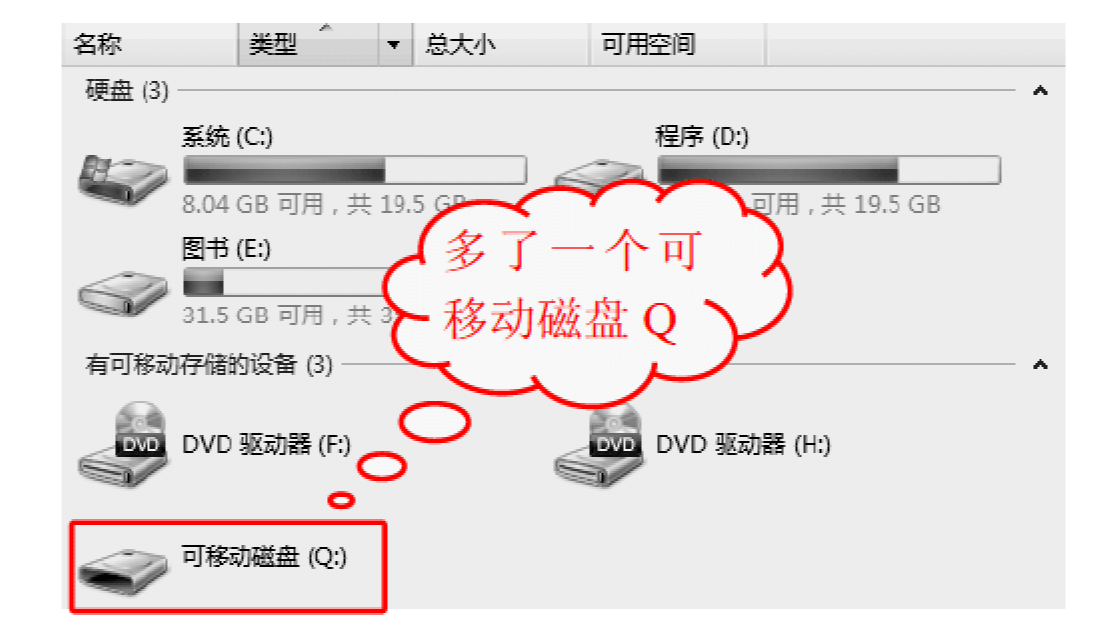












注　意　事　项

输入密码时，密码长度不能短于 5 个字符，否则会提示重新输入，创建的虚拟加密磁盘容量不要大于文件所在磁盘的容量。

(2) 隐藏虚拟加密磁盘

Dekart Private Disk 使用美国标准算法 AES 和 SHA-1 算法技术，通过设置可以使它隐藏进行。



❸ 断开虚拟加密磁盘后，可以发现可移动磁盘 Q 消失了。

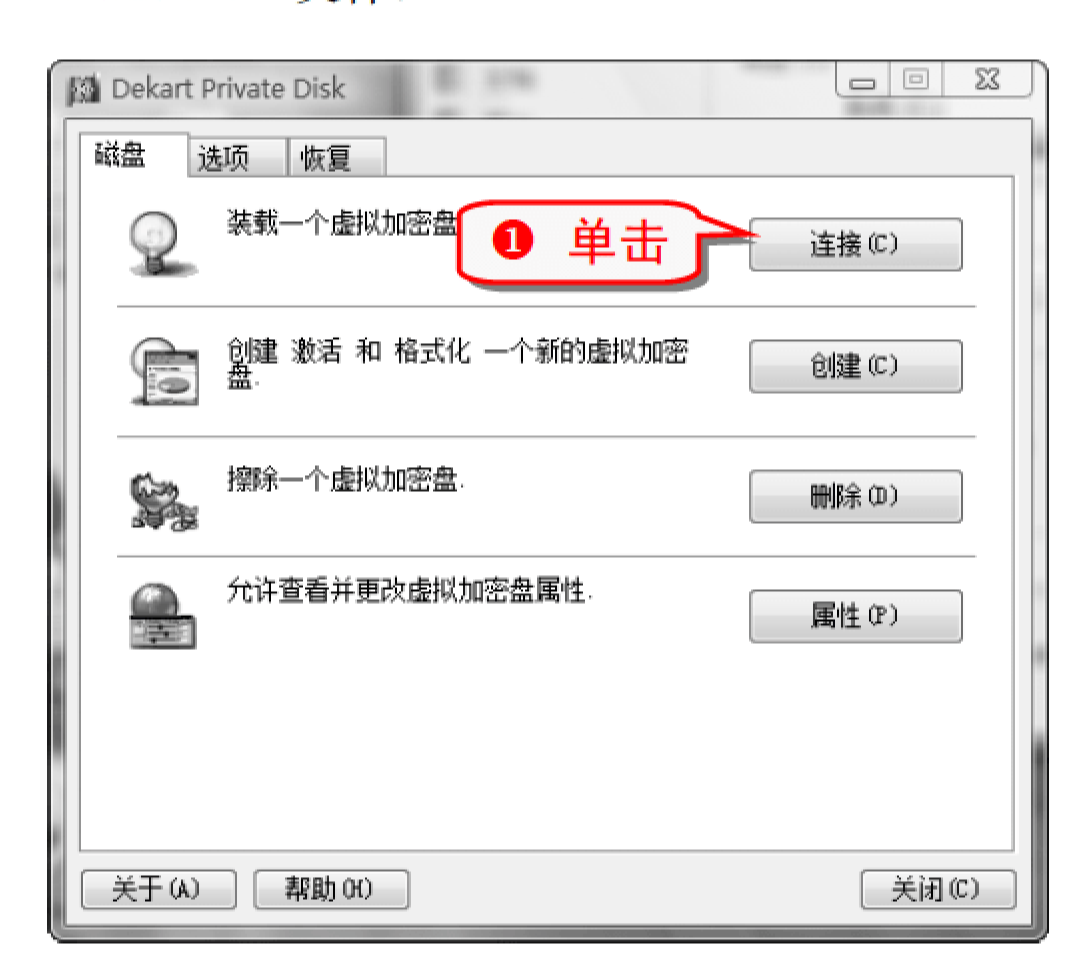


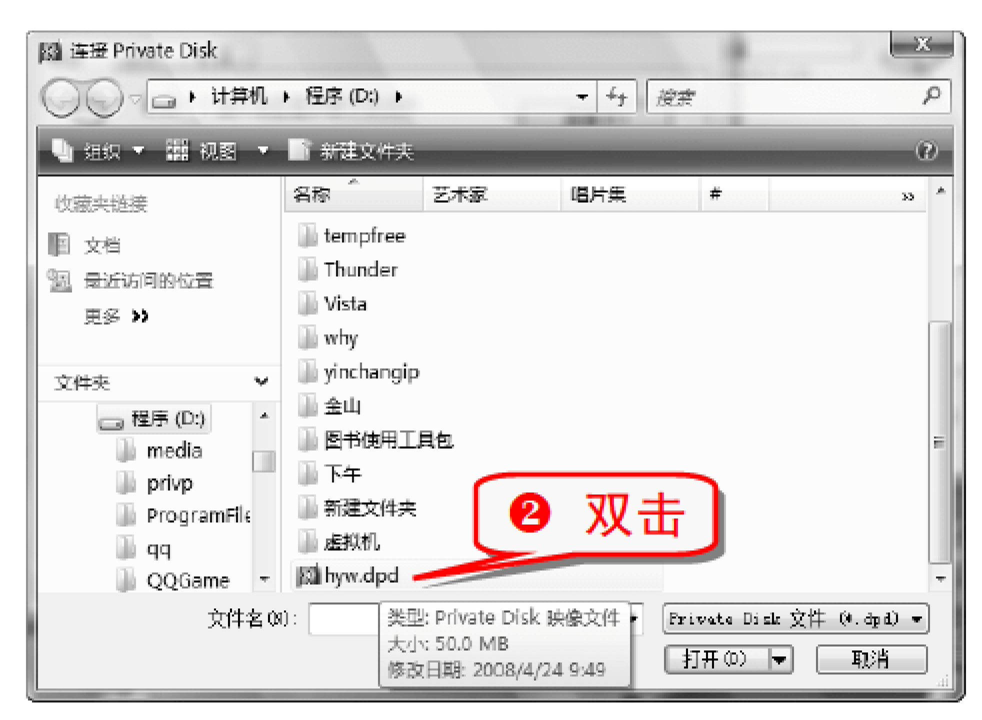


按下 Ctrl + F12 组合键可以快速关闭所有虚拟加密盘，按下 Ctrl + Alt + F12 组合键可以在关闭所有虚拟加密盘的同时退出 Dekart Private Disk 程序。

(3) 打开虚拟加密磁盘

打开虚拟加密磁盘比较简单，双击解压文件类中的“PrvDisk.exe”文件。





(4) 虚拟磁盘的备份

通过对虚拟磁盘的备份，可以创建压缩的、加密的、带密码保护的虚拟加密副本。









(5) 虚拟磁盘的恢复

使用虚拟磁盘的修复功能，可以从以前创建的虚拟加密盘副本里恢复数据。











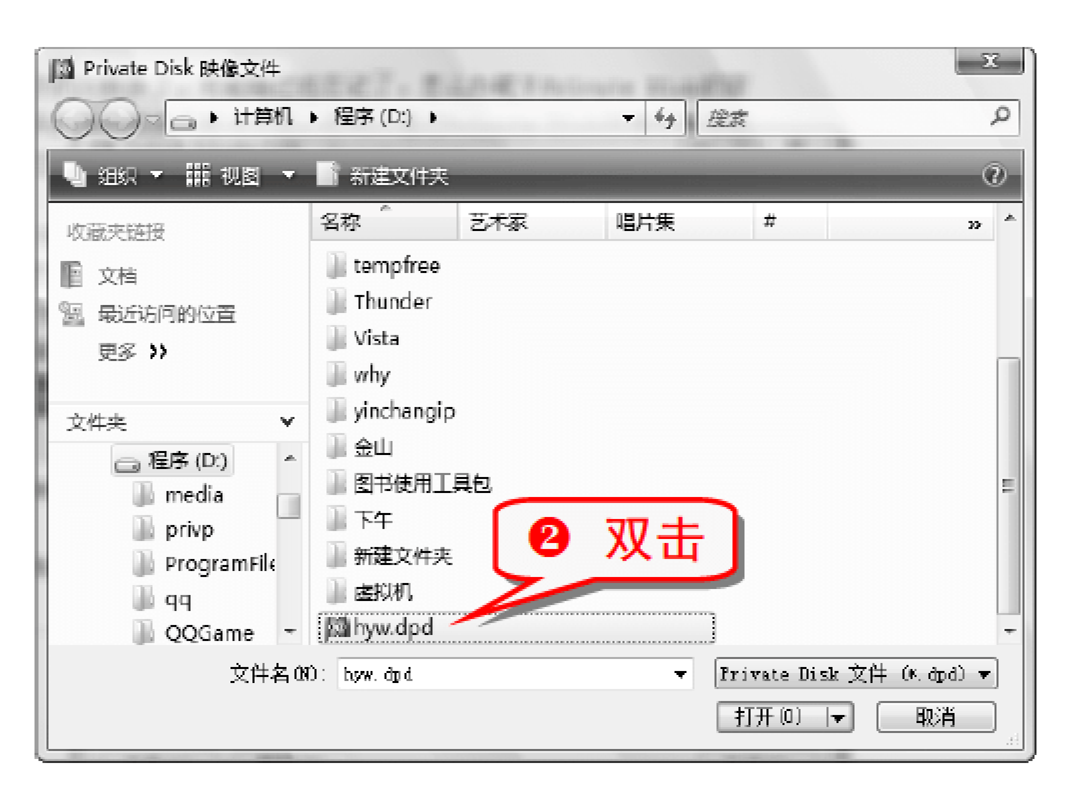
注　意　事　项

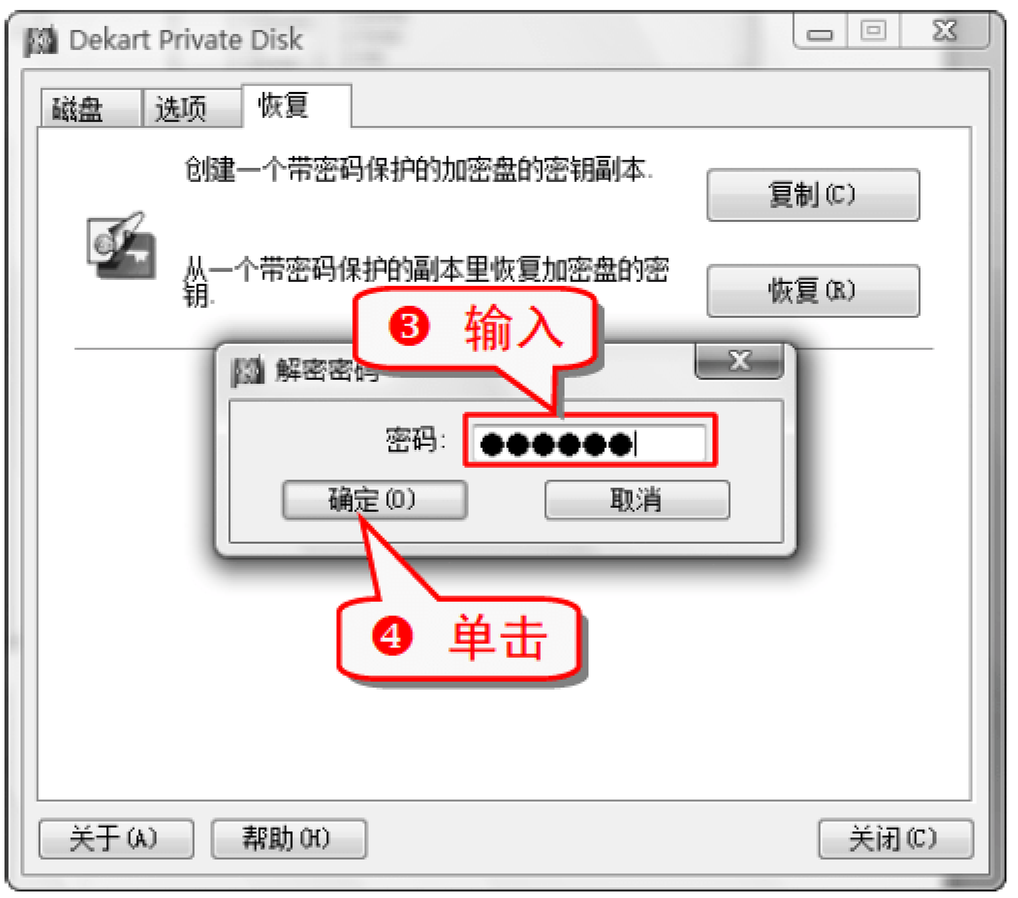
虚拟加密磁盘如果是只读磁盘，就不能对其进行恢复。

(6) 密码的备份

通过对密码的备份操作，可以创建一个带密码保护的加密盘的密钥副本。





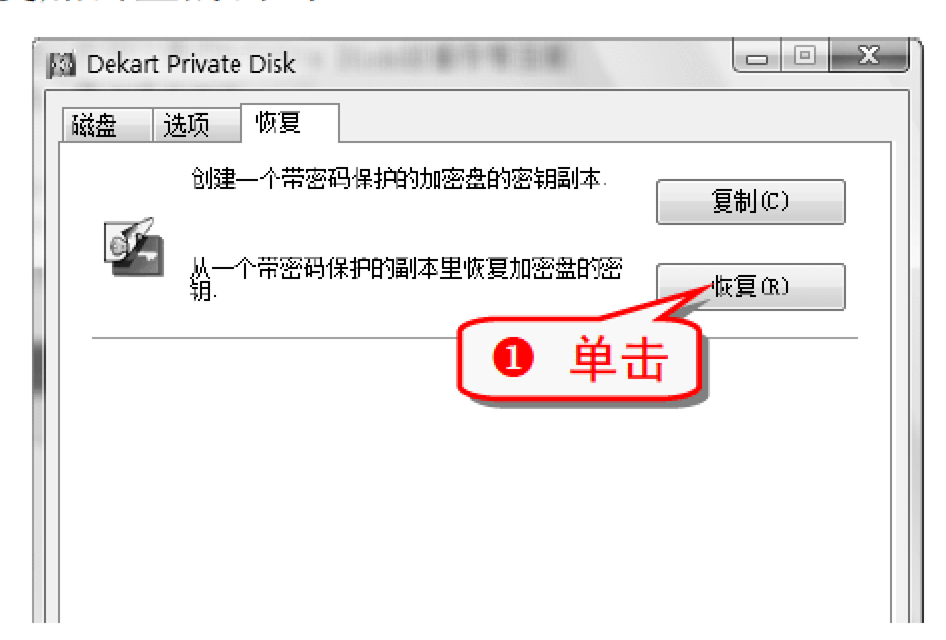






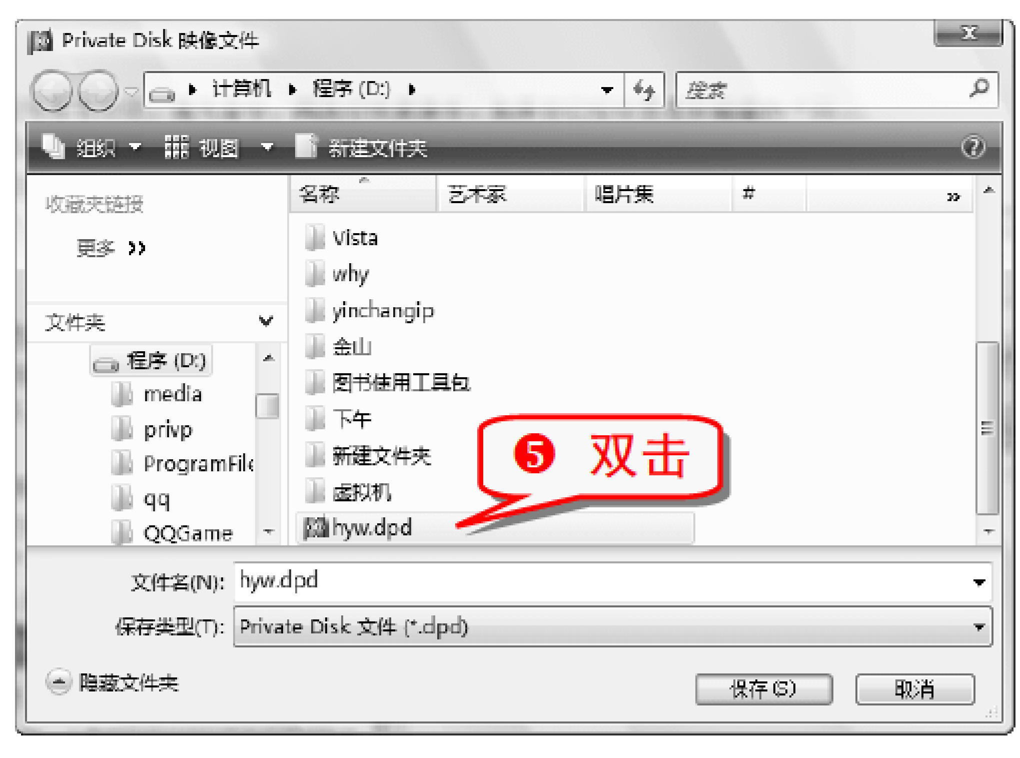
(7) 密码的恢复

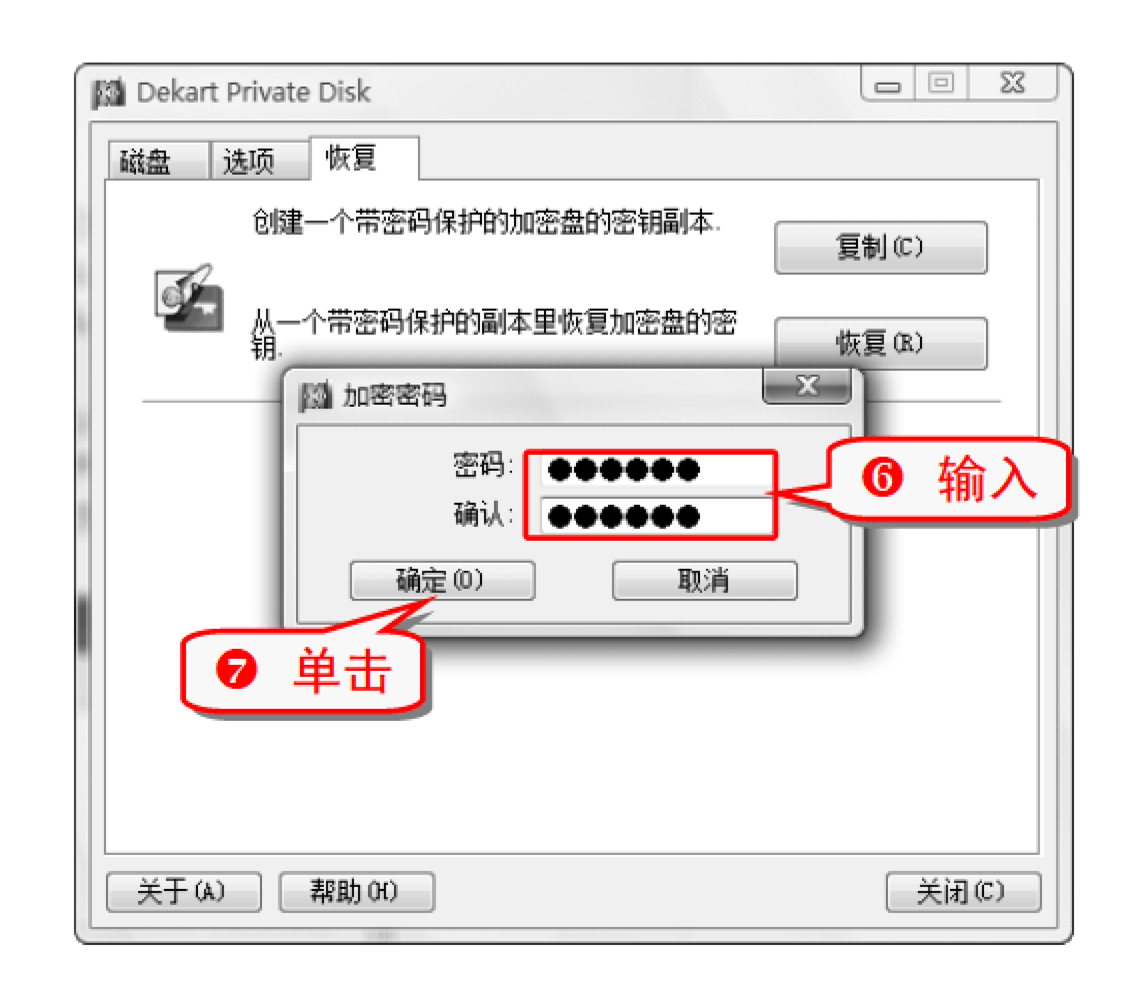
使用密码的恢复功能，可以从一个带密码保护的副本里恢复加密盘的密码。









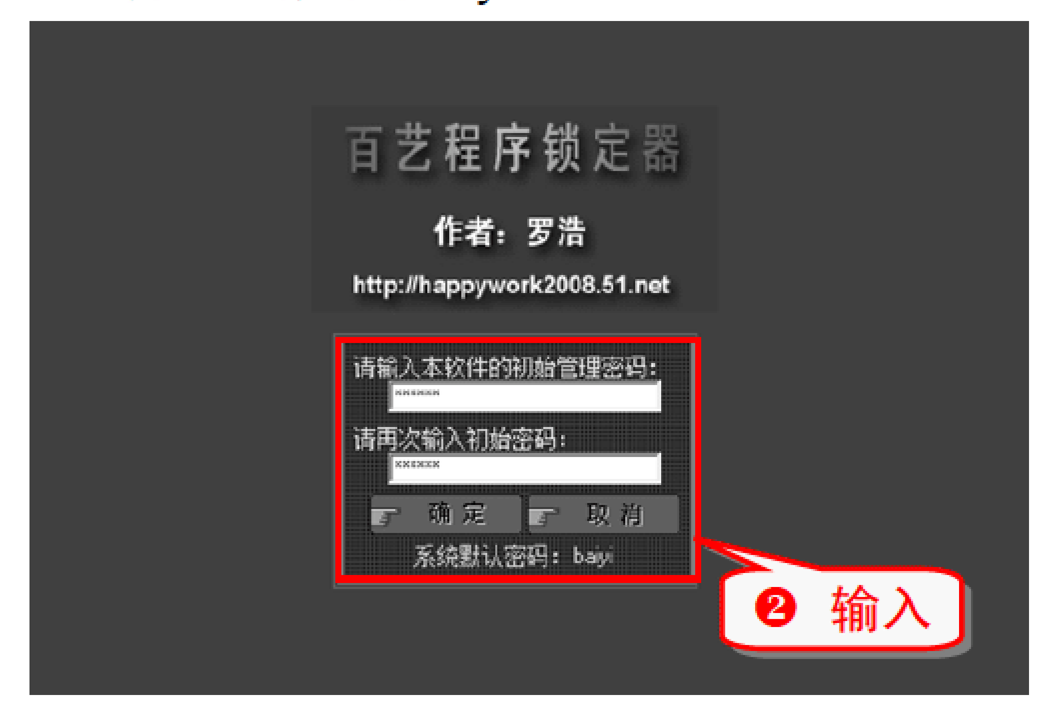


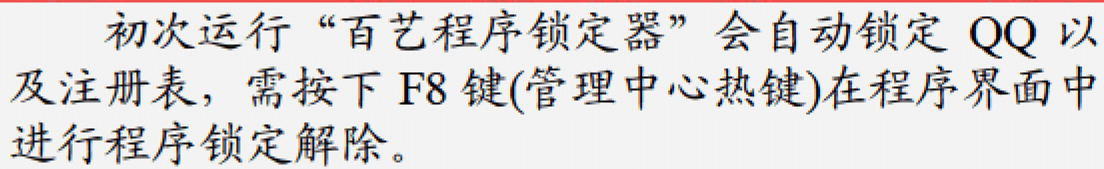
技巧91 巧用百艺程序锁定器给电脑加密

百艺程序锁定器功能强大，可以将程序定时进行锁定，对于在 Windows 环境下运行的程序，只要找到运行程序文件，就可以进行锁定设置。

(1) 设置密码

❶ 安装该软件会出现程序欢迎界面以及初始密码设置框，其默认密码是 baiyi。





初次运行“百艺程序锁定器”会自动锁定 QQ 以及注册表，需按下 F8 键(管理中心热键)在程序界面中进行程序锁定解除。

安装完成后，运行百艺程序锁定器会弹出如下对话框，需要输入密码才能使用该软件。

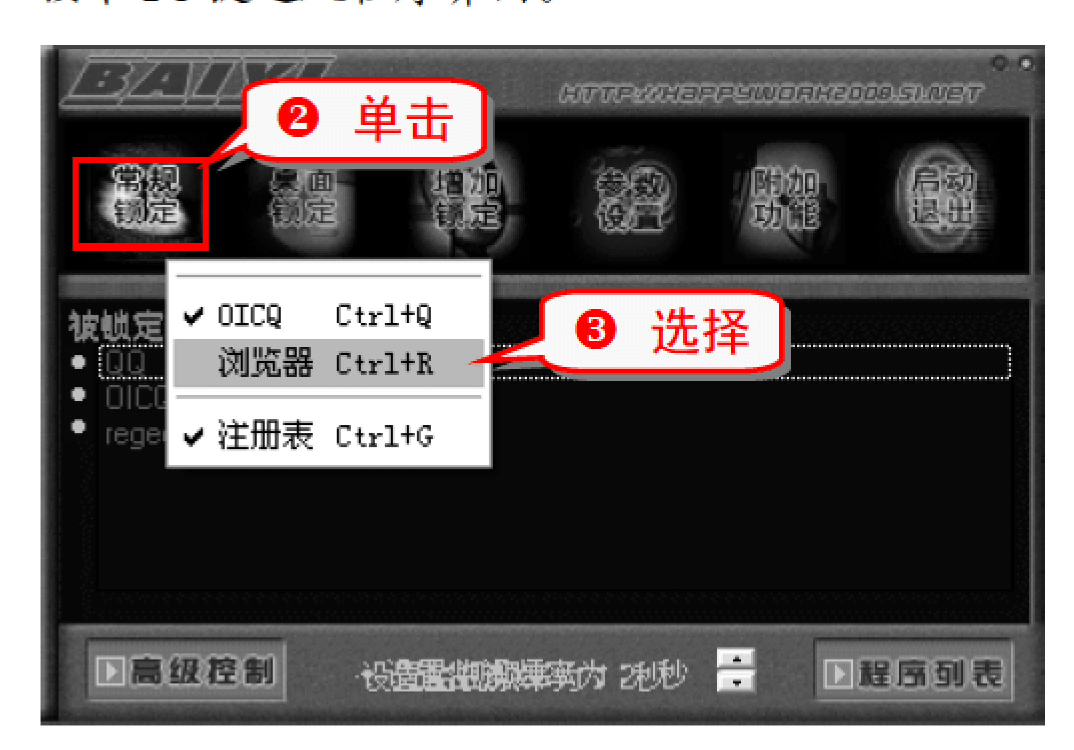




(2) 常规锁定

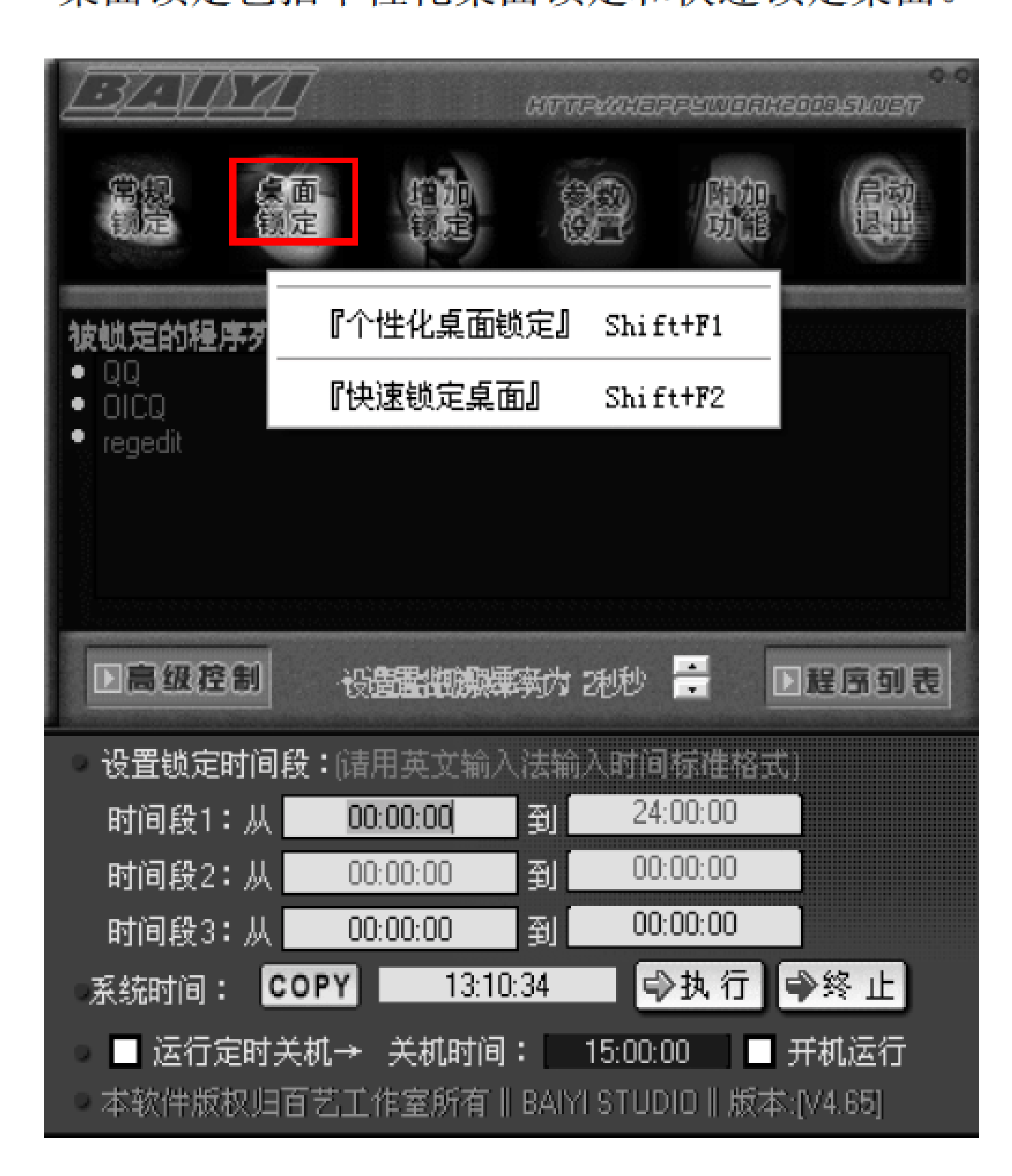
QQ 和注册表在默认情况下是自动锁定的，在常规锁定中有 QQ、浏览器和注册表锁定，浏览器默认情况下是不锁定的，下面介绍锁定浏览器的方式。

❶ 按下 F8 键进入程序界面。



(3) 桌面锁定

桌面锁定包括个性化桌面锁定和快速锁定桌面。



❶ 选择个性化桌面锁定，会跳出一个“锁定界面个性设置”对话框，在该对话框中可以设置桌面锁定时的背景桌面图像、文字提示，可以更改文字提示的样式、大小、颜色使其与系统相应的提示相适应。



❷ 设置完以后单击“现在锁定”按钮，出现的效果图如下。



❸ 选择快速锁定桌面，桌面会立即被锁定，屏幕变成黑色，右下角有个输入密码的文本框，用来解除锁定。效果如下图所示。



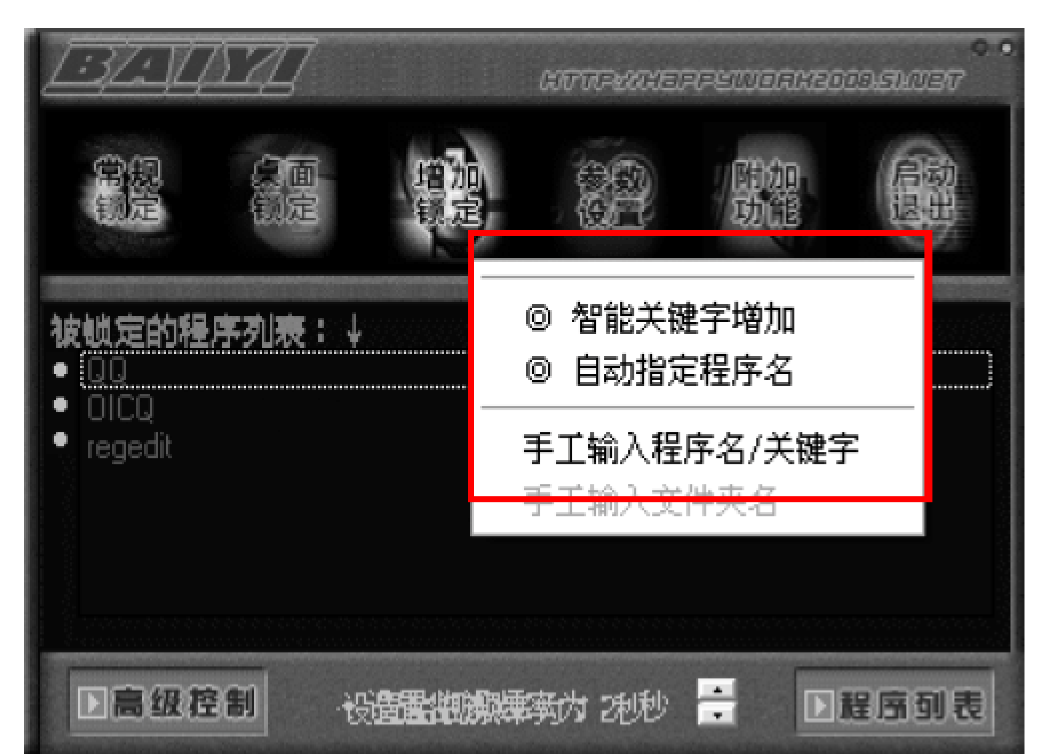
(4) 增加锁定

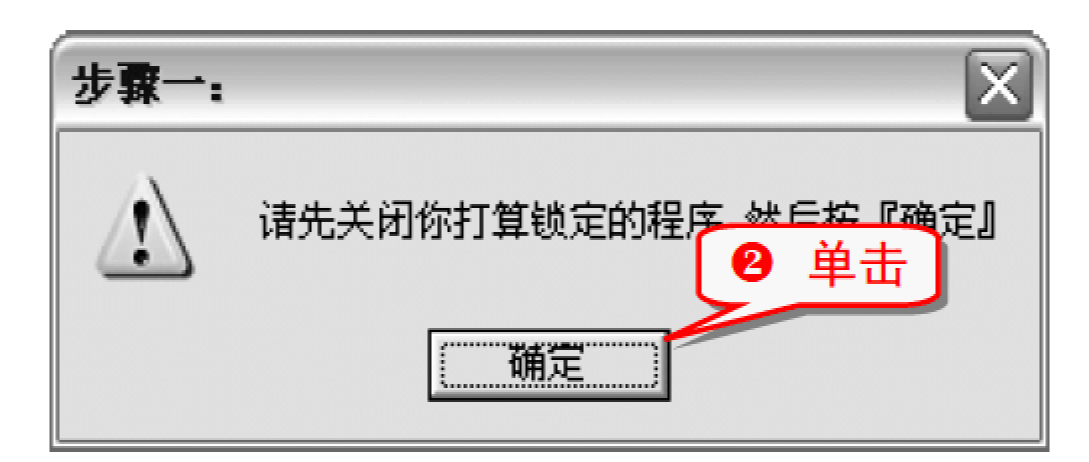
当要增加锁定的程序时，可以选择“增加锁定”选项，它包含四个子选项。

- 智能关键字增加：提示用户首先关闭要锁定的程序，然后单击“确定”按钮。
- 自动指定程序名：弹出浏览对话框，选择要锁定的程序。
- 手工输入程序名/关键字：输入程序名或程序关键字锁定相关程序。
- 手工输入文件夹名：手工输入要锁定的文件夹名称。

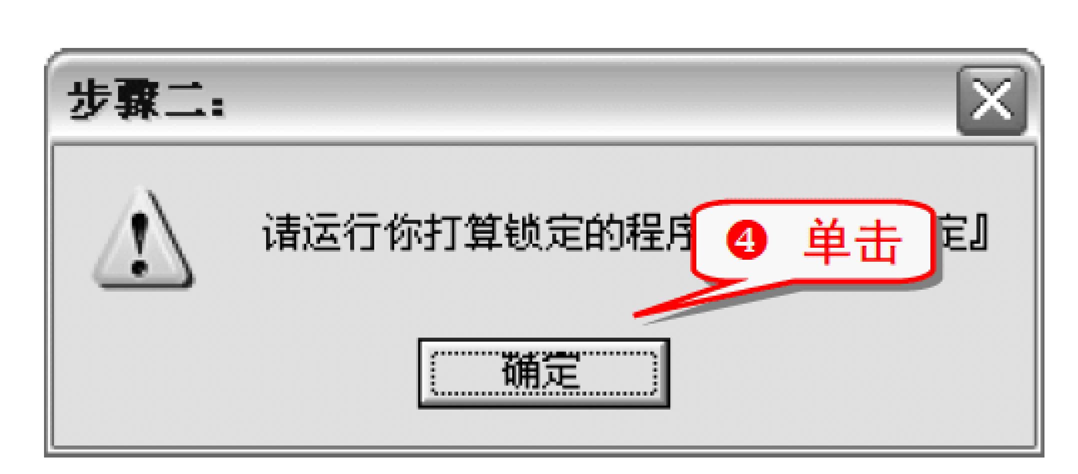
下面以“智能关键字增加”选项的使用为例，学习如何将 Media Player 增加到锁定列表中。

❶ 选择“增加锁定”→“智能关键字增加”命令。





❸ 运行 Media Player 程序。





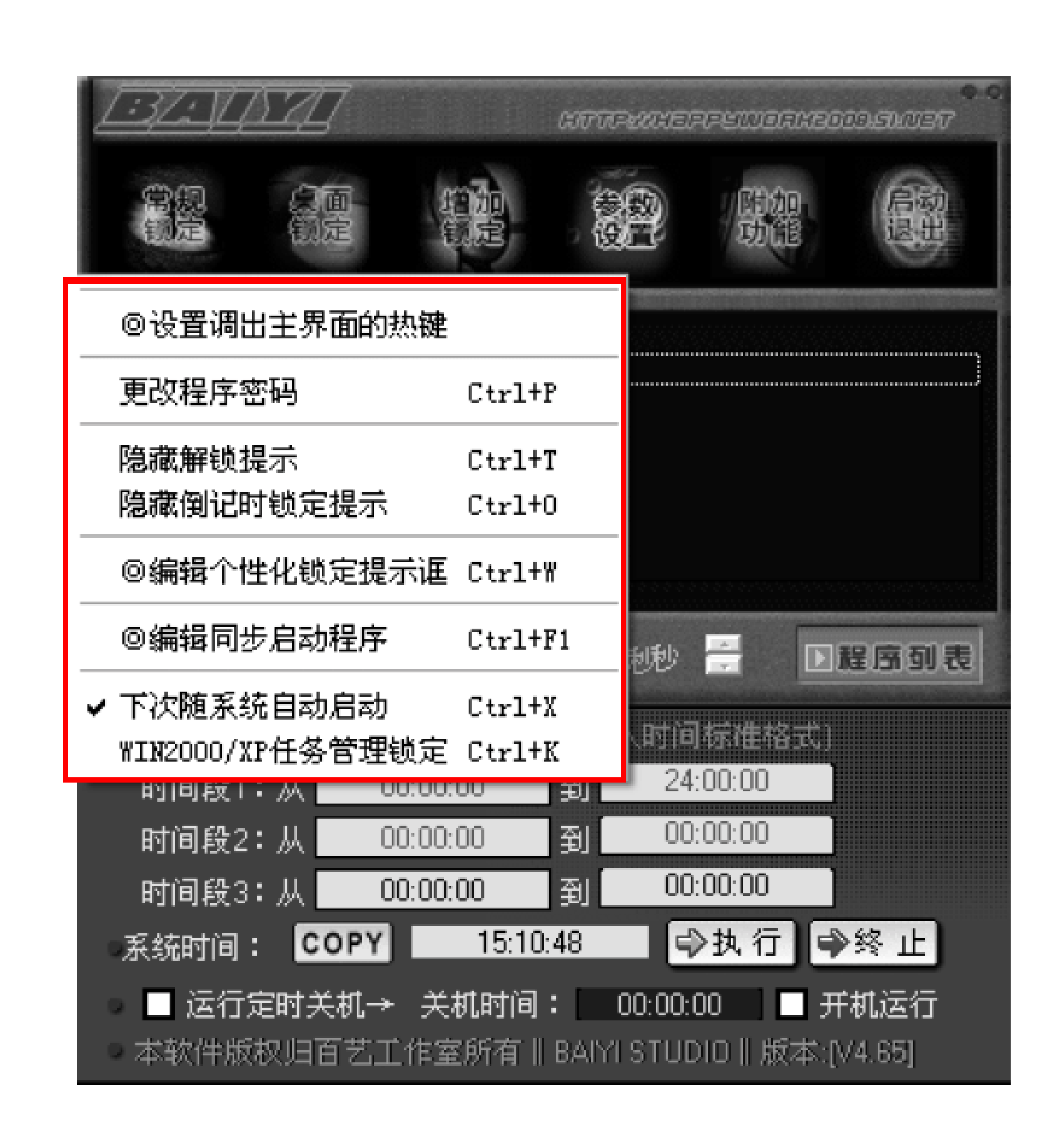


❼ 锁定的程序列表中多了一个 wmplayer 项，Media Player 程序不能运行了。



(5) 参数设置

百艺程序锁定器主界面的“参数设置”选项中有 8 个子选项。



其中“编辑个性化锁定提示框”子选项用于为锁定的程序设置个性化提示，提示对话框的标题、内容以及图标都可以改动。

下面介绍怎么为注册表设置个性化锁定提示框。

❶ 选择“参数设置”→“编辑个性化锁定提示框”命令。

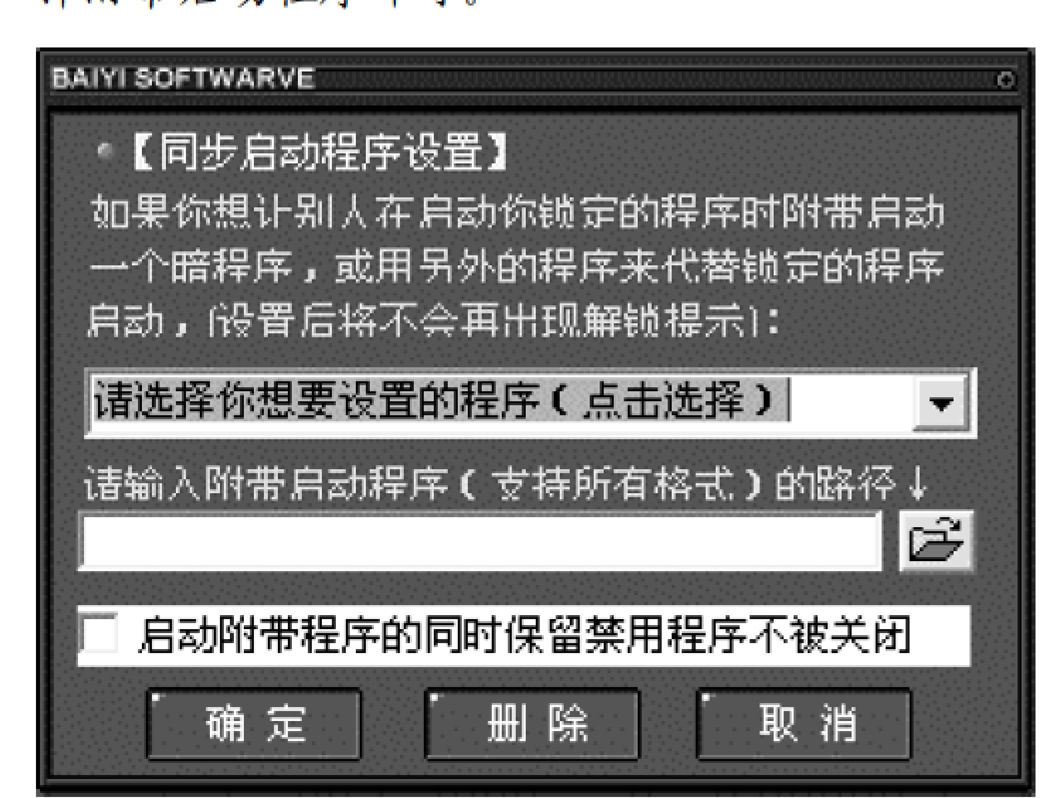




❻ 设置完以后尝试打开“注册表编辑器”窗口，弹出如下图所示的提示框。

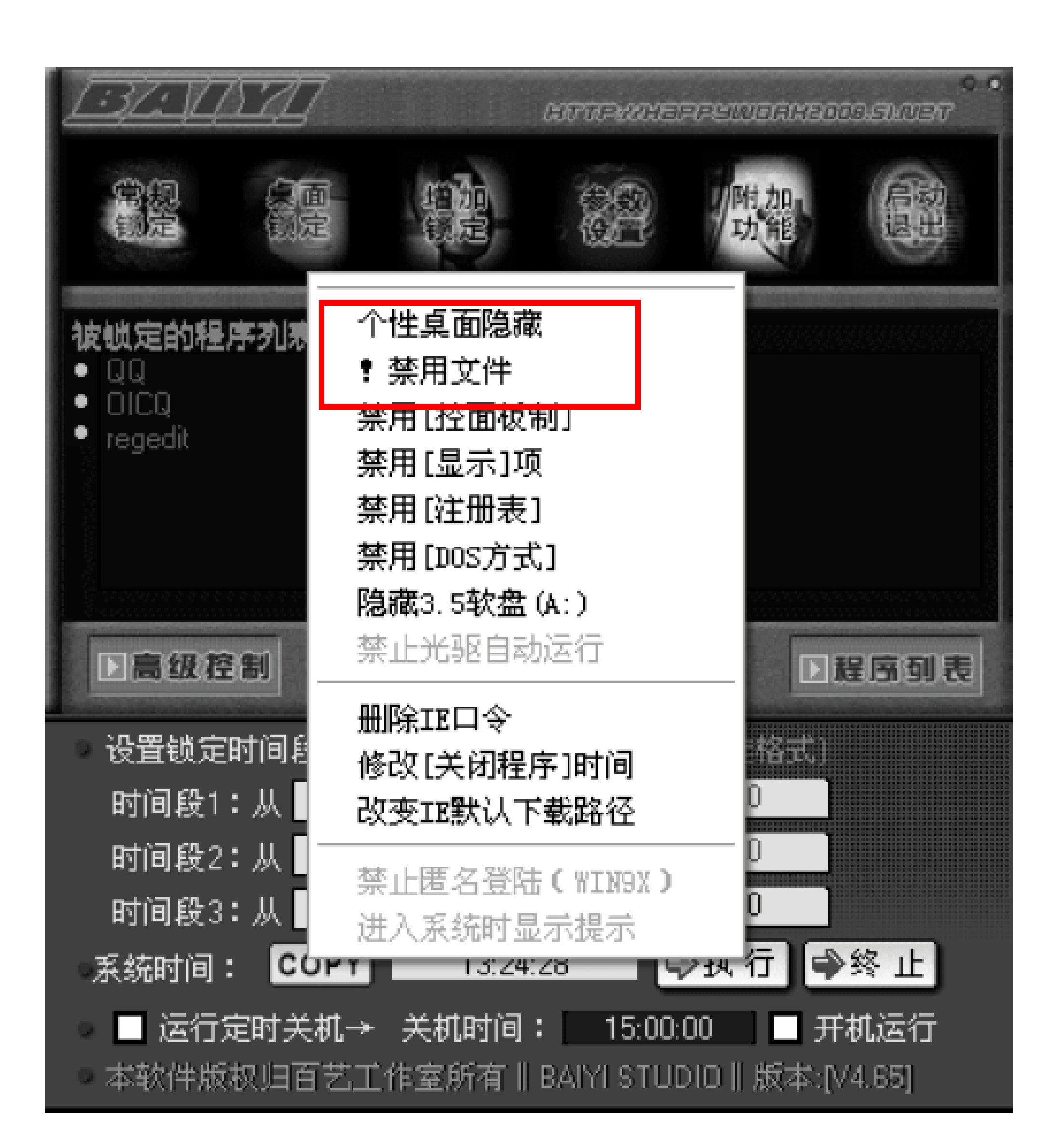


❼ 为被拦截的程序设置同步启动程序，只要在“同步启动程序设置”界面里先选择要设置的程序，然后再选择附带启动程序即可。

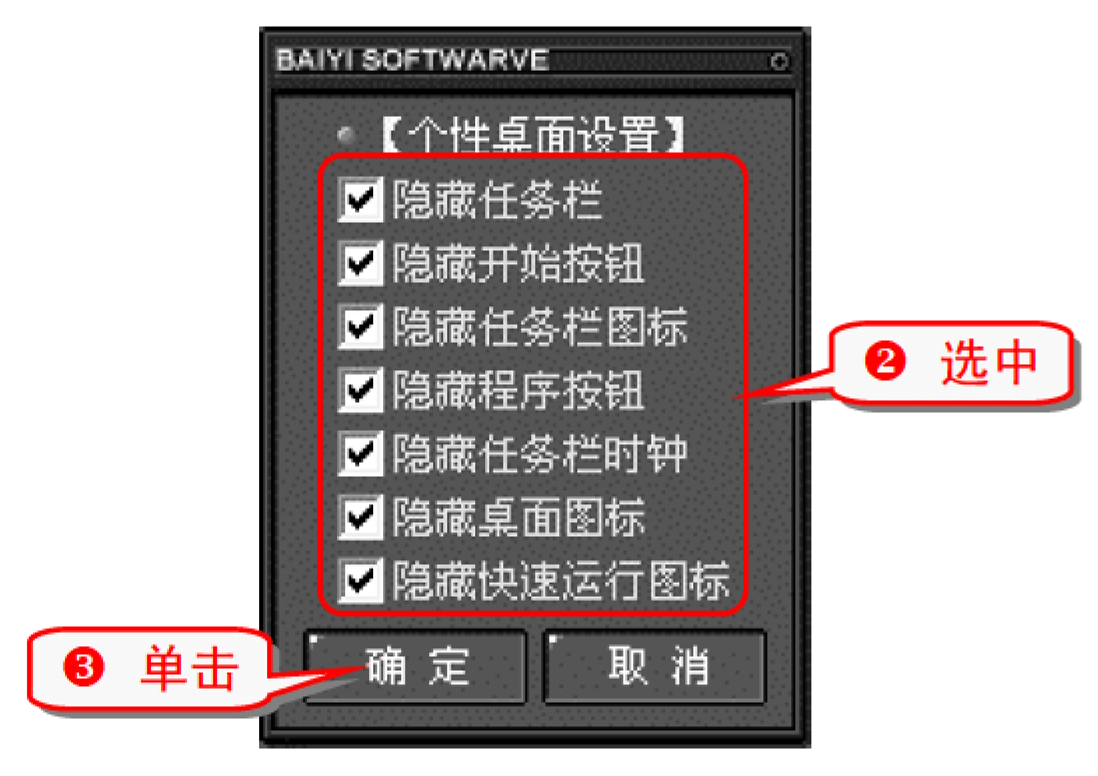


(6) 附加功能

“附加功能”选项中包含禁用“控制面板”、禁用“显示”项、禁用“注册表”以及修改“关闭程序”时间等很多功能，最有实用价值的是“个性桌面隐藏”与“！禁用文件”两项。



❶ 选择“个性桌面隐藏”命令，弹出一个“个性桌面设置”界面。



❹ 选择“！禁用文件”命令，弹出“设置禁用文件”界面，通过单击“增加”按钮添加禁用的文件，通过单击“删除”按钮取消禁用的文件。



 注 意 事 项 

被禁用的文件不能对其进行访问、修改以及删除等任何操作。设置禁用文件以后，必须重新启动电脑才有效。

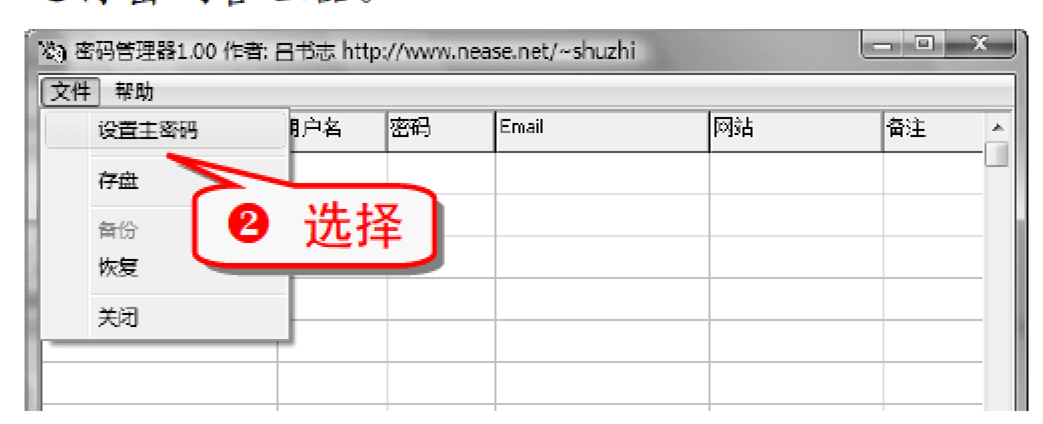
 知 识 补 充 

百艺程序锁定器在电脑开机时会自动运行，按下F8 键会弹出程序运行界面。百艺程序锁定器不支持Windows Vista 系统。

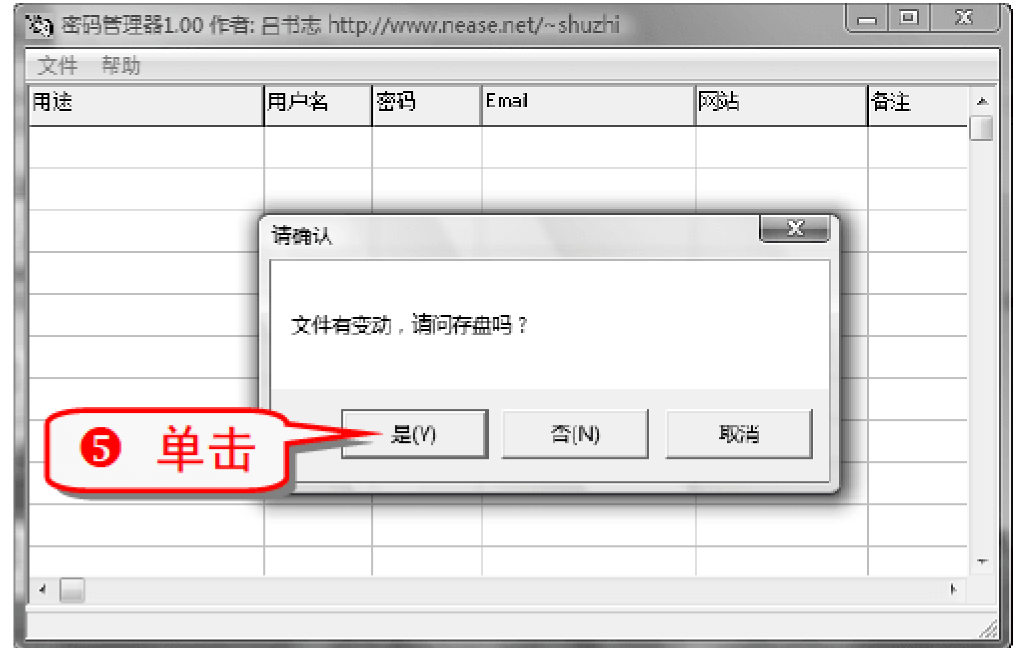
技巧92 为密码找个管家

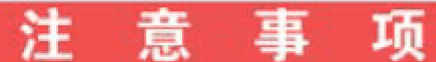
随着网络的发展，电脑的普及，用户设置的密码也越来越多，经常会出现密码遗忘等问题。可以用软件来管理所有的密码。密码管理器下载后可以直接运行。

❶ 运行密码管理器。







 注 意 事 项 

主密码一定要牢记，不能丢失。



专题四　找回丢失的密码

内容导航

设置密码能很好地保护电脑中的重要文件，就好比给电脑加了“防盗门”，握有正确的“钥匙”才能开启这扇门。由于设置的密码太多，很多密码被遗忘，找回遗失的密码变得很重要。

热点快报

- 破解 CMOS 密码
- 破解屏幕保护密码
- 找回 QQ 密码技巧
- 破解 QQ 空间密码
- 使用密码查看器技巧
- 制作密码重置盘

技巧93　两招破解电脑 CMOS 密码

下面介绍两种实用的破解 CMOS 密码的方法。

(1) 用 Debug 命令破解

❶ 在电脑的第一启动选项是 CD-ROM 的前提下，插入一张启动盘(如 Windows 98 的操作系统光盘)，重新启动电脑后进入 DOS 状态。

❷ 输入 Debug 命令后按下 Enter 键。

❸ 输入以下命令。

```
-o 70 11
-o 71 FF
-q
```

❹ 重新启动电脑，按 Delete 键进入 BIOS 设置界面，重新设置 BIOS 选项。

(2) CMOS 放电法

❶ 拔掉电源线，打开电脑机箱。

❷ 找到主板上的纽扣电池，将其取下放置几分钟后使其放电。

❸ 将电池重新装上，合上机箱，然后插上电源线。

❹ 开机后，按 Delete 键进入 BIOS 设置界面，重新设置 BIOS 选项。

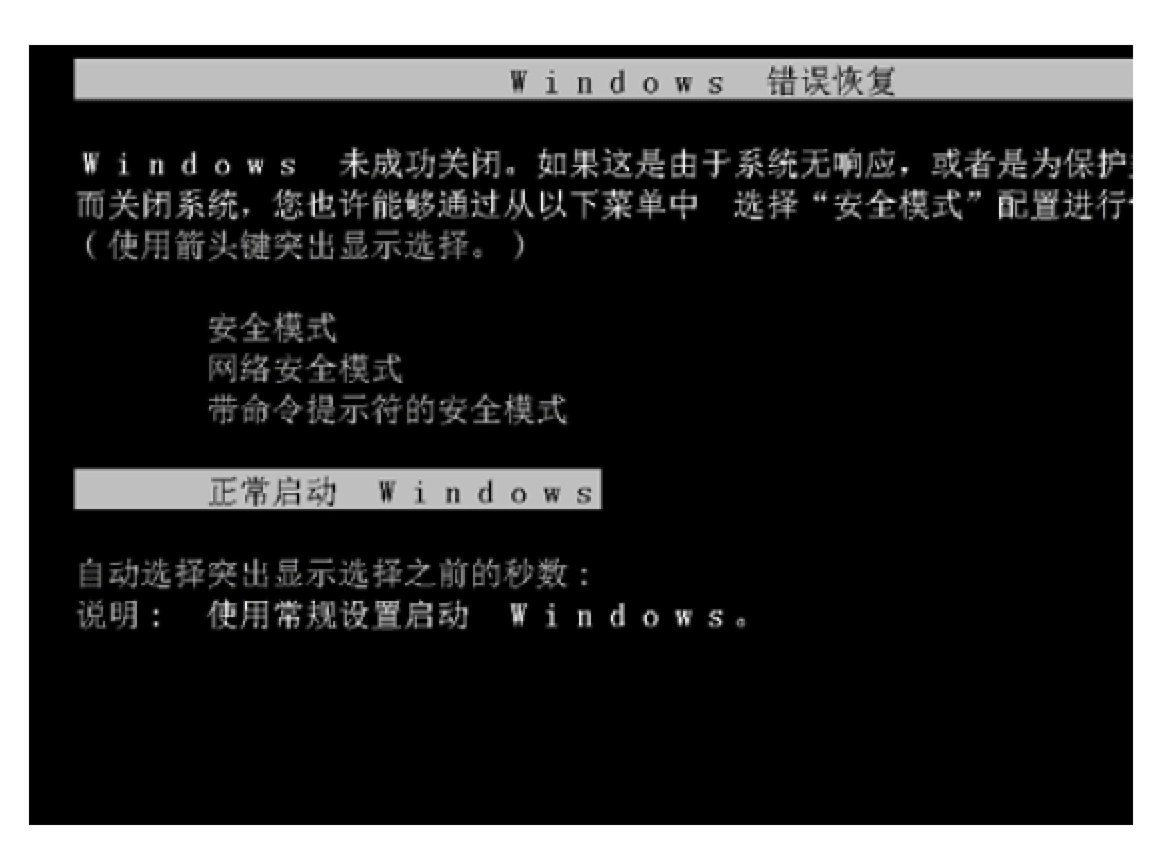
技巧94　重新启动电脑破除屏幕保护密码

破除屏幕保护密码最简单的方法就是重新启动电脑。

❶ 下图是电脑进入屏幕保护时的状态。



❷ 按下机箱上的重新启动按钮，重新启动电脑进入如下界面。



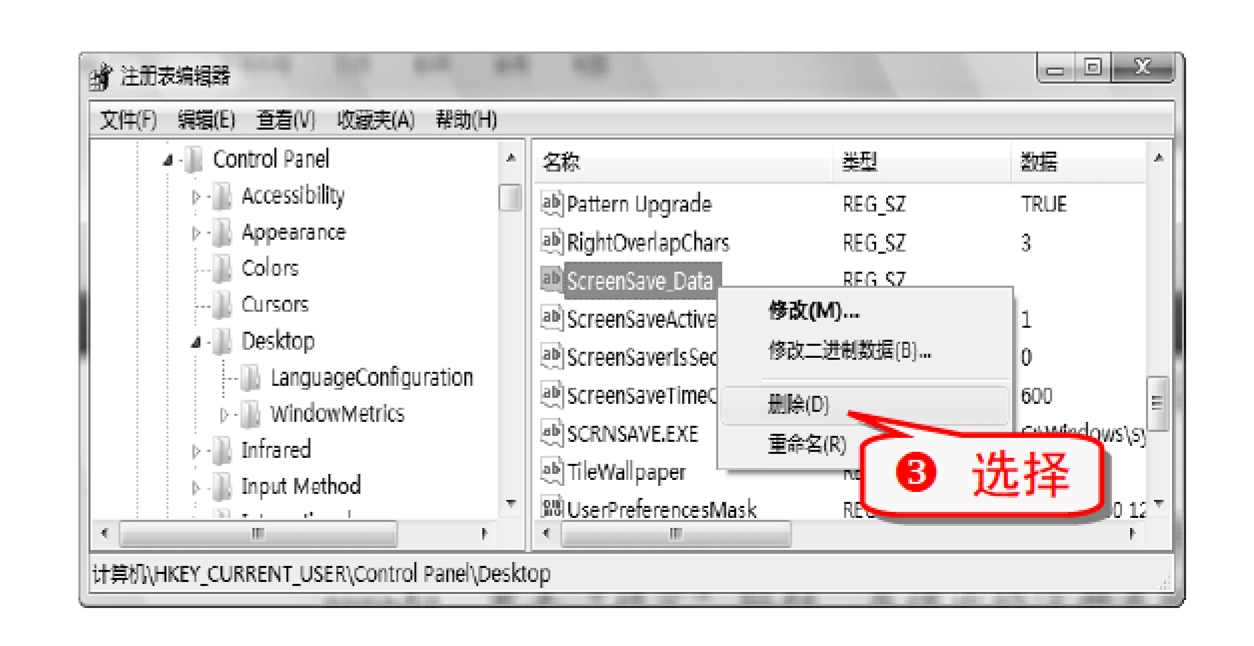
❸ 按下 Enter 键进入系统。

技巧95 删除屏幕保护密码

设置过屏幕保护密码，但是密码被忘记了，此时可以通过修改注册表来删除屏幕保护密码。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\ControlPanel\Desktop\ScreenSave_Data 分支。

❷ 在右边窗格中选中 ScreenSave_Data 后右击。

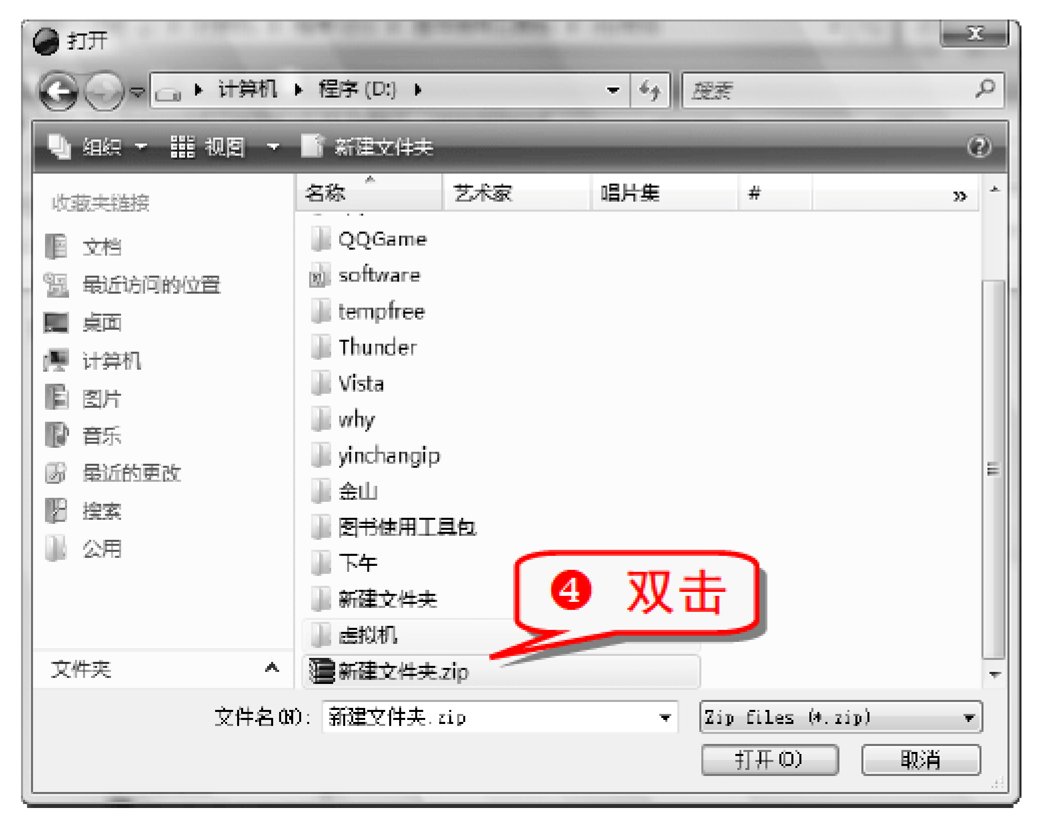


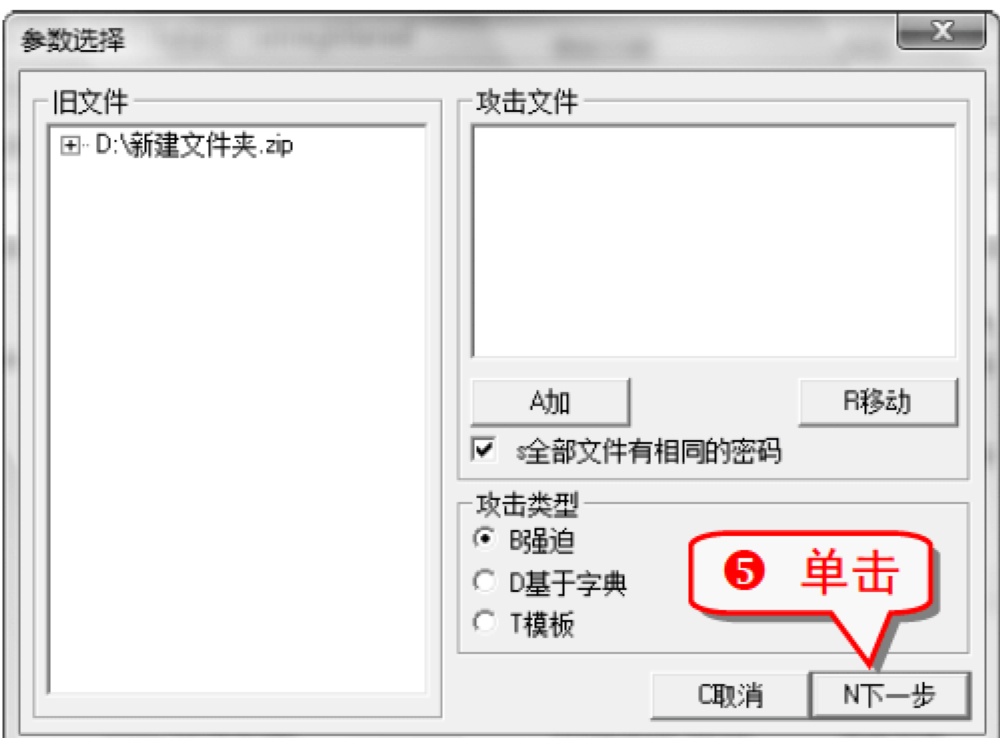
技巧96 找回 WinZIP 文件的密码

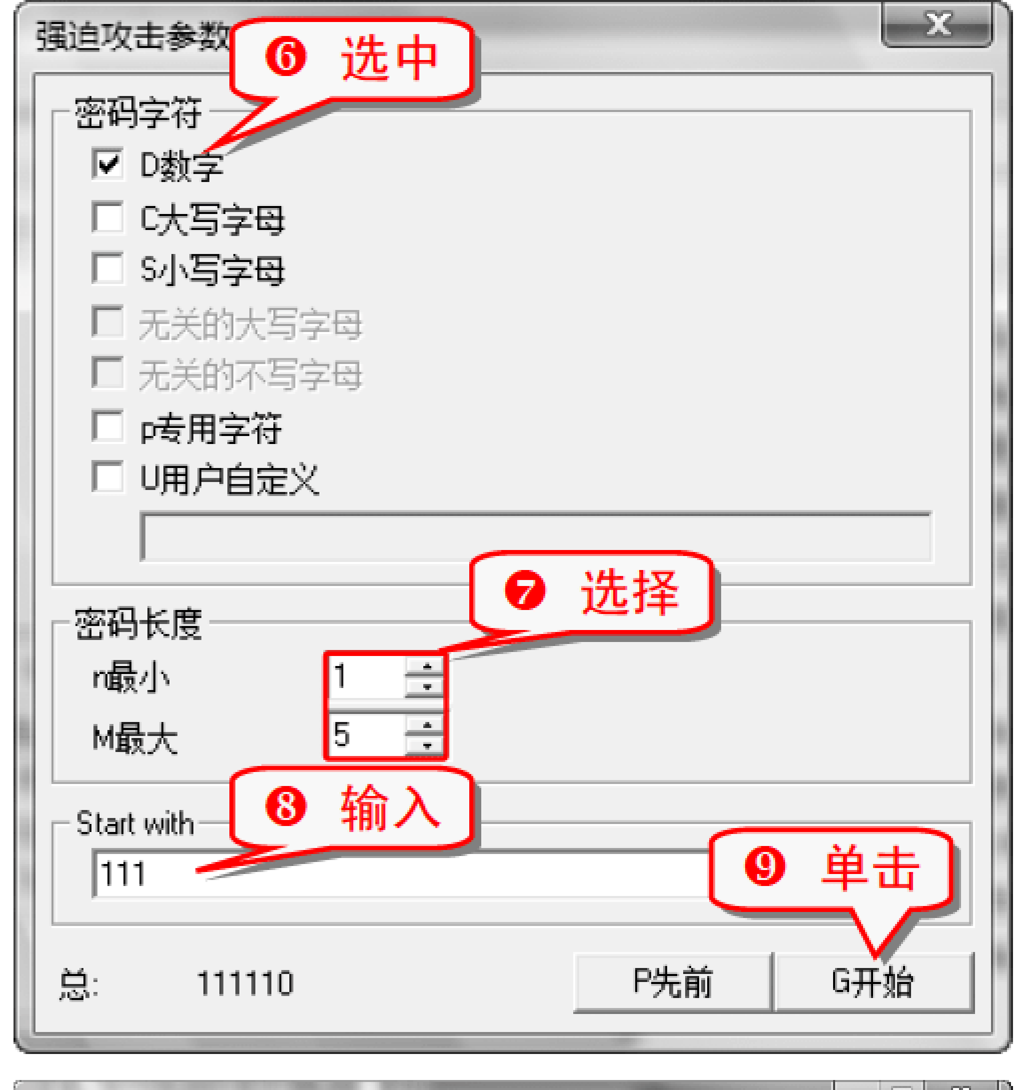
网上有很多破解 WinZIP 密码的工具，UZPC 软件是比较好的一个工具。

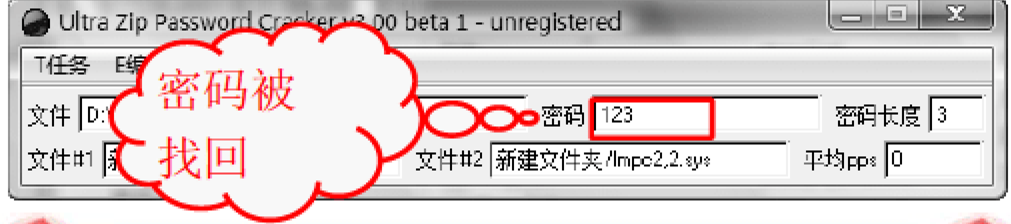
❶ 打开 UZPC 主界面。











注 意 事 项

密码长度、密码字符和开始密码选得越精确，找回密码的时间也就越快。

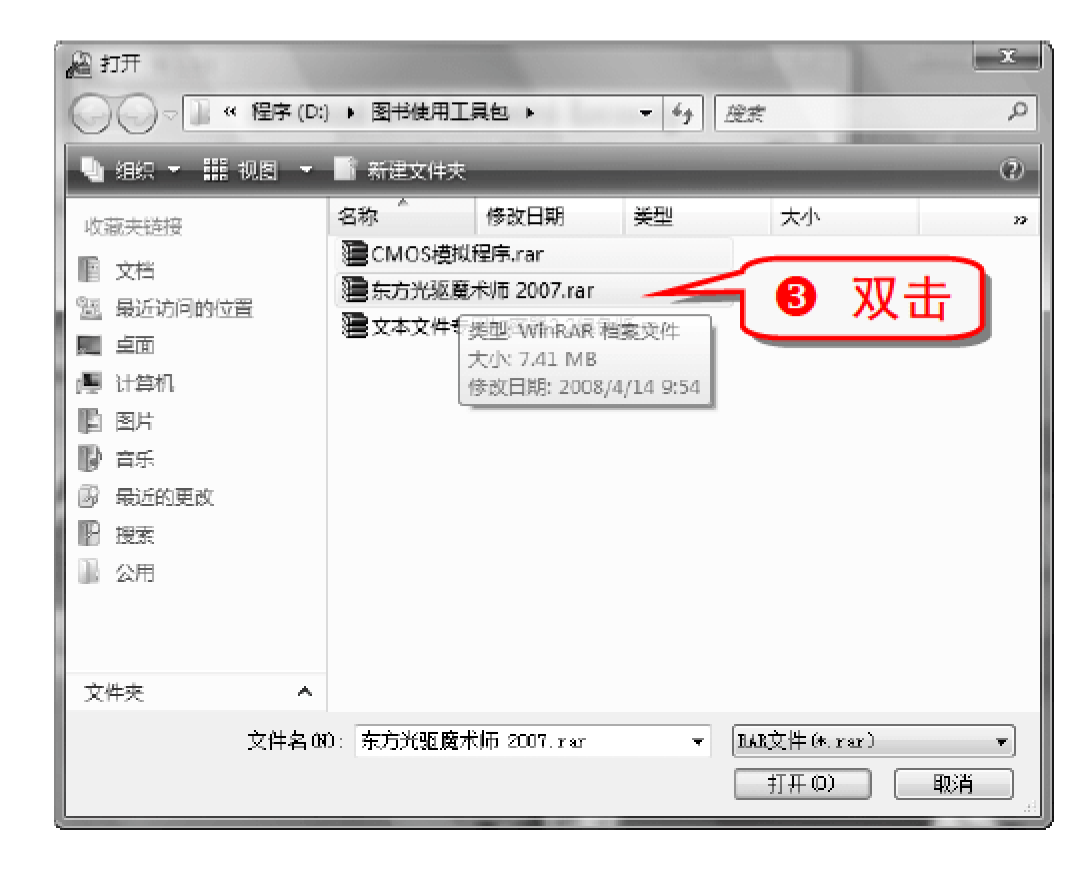


技巧97　找回 WinRAR 文件的密码

使用 ARPR 密码破解软件可以找回 WinRAR 加密文件的密码。

❶ 打开 ARPR 1.53 主界面。









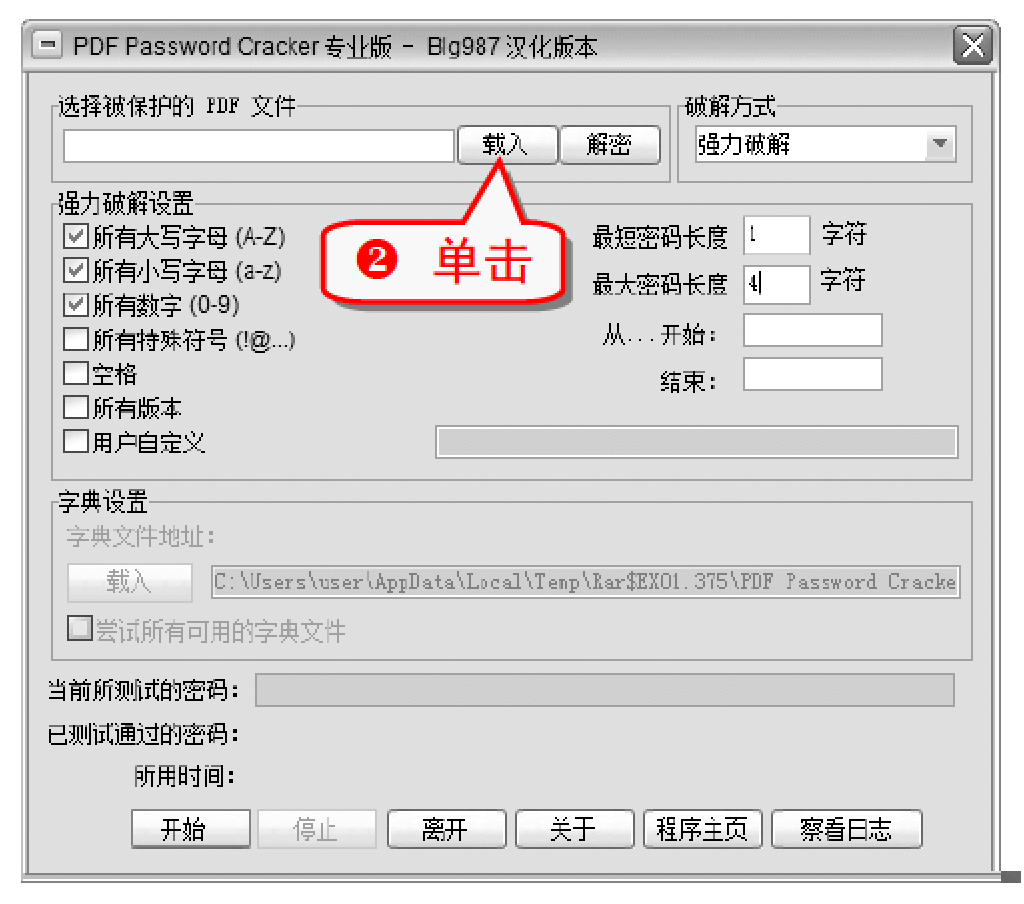
注　意　事　项

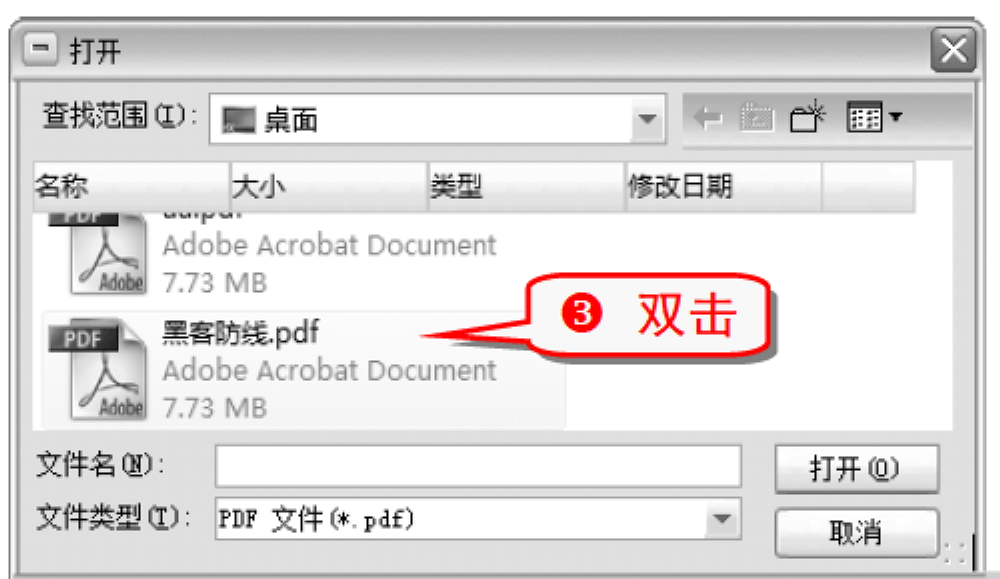
这种方法很浪费时间，选择密码范围时，要尽量缩小密码的范围。

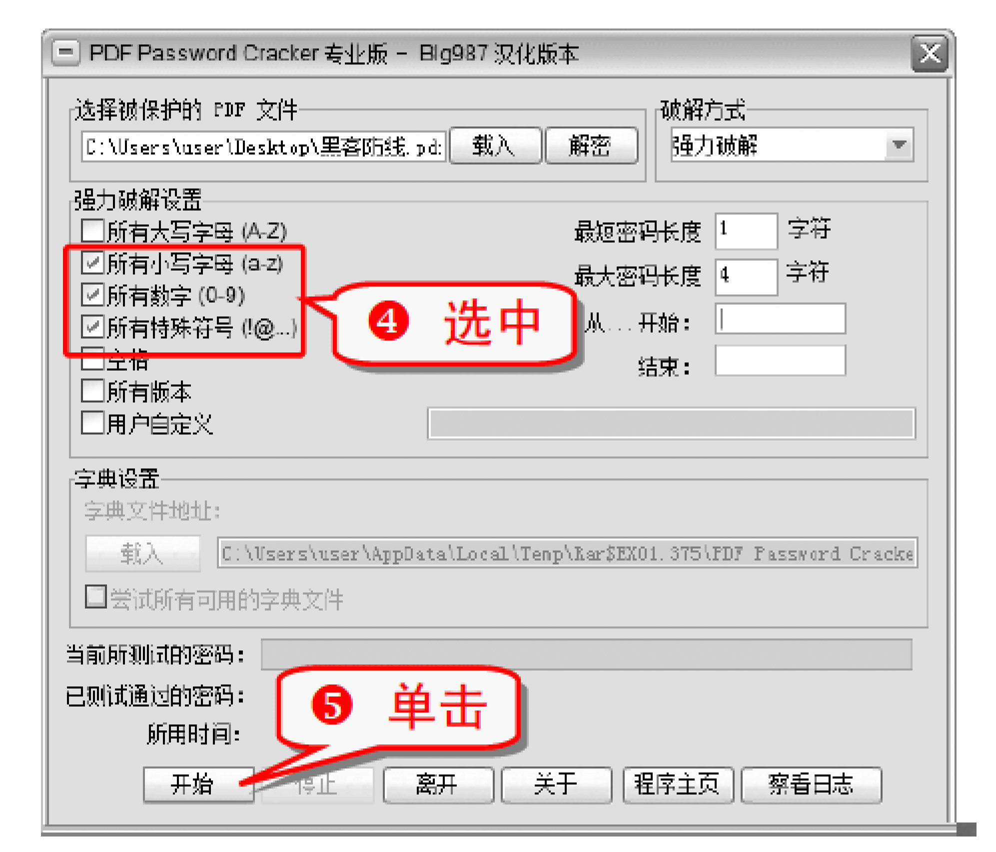
技巧98　找回 PDF 文档的密码

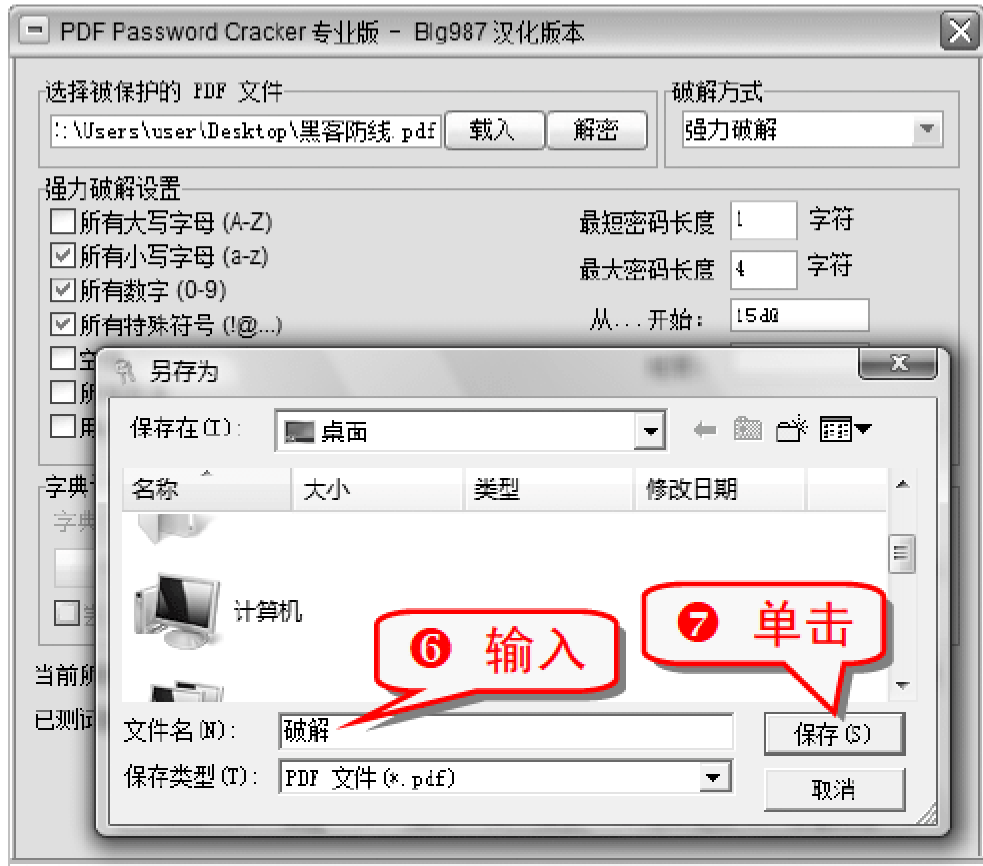
使用 PDF Password Cracker 密码破解软件可以找回 PDF 文档的用户级密码。

❶ 打开 PDF Password Cracker 专业版主界面。









技巧99 两招找回 QQ 密码

拥有 QQ 号码较多，会出现遗忘密码的问题，想要找回密码很简单。

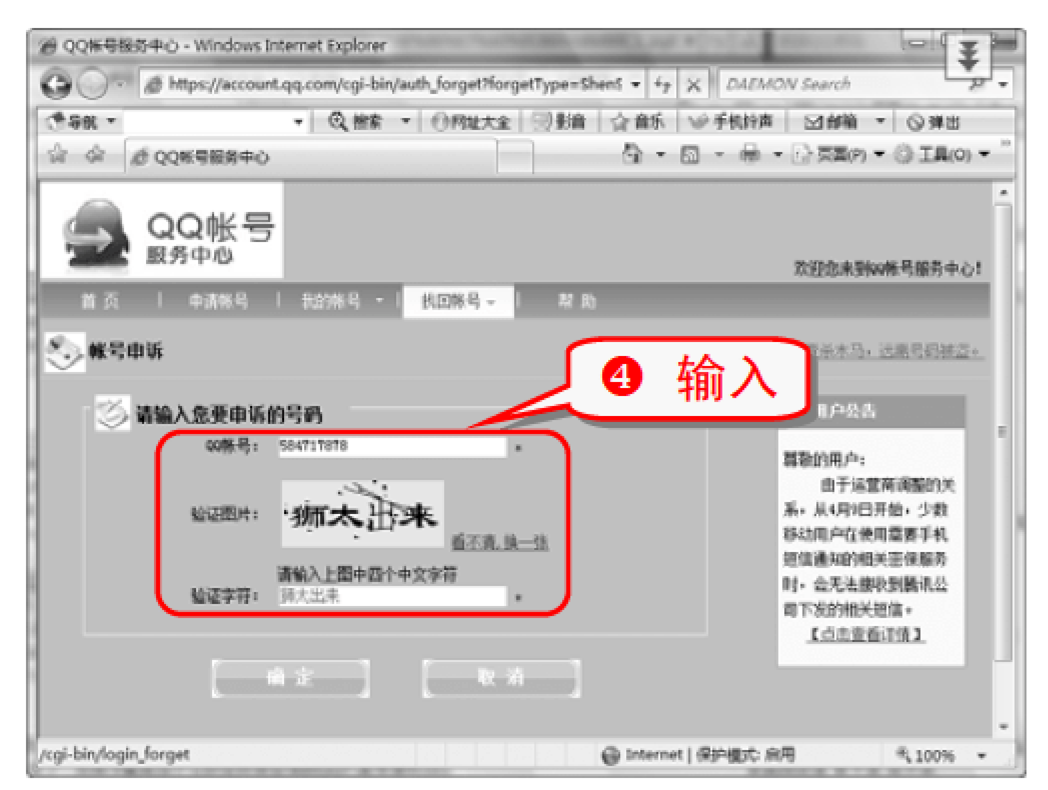
(1) 忘记密码保护的情况下

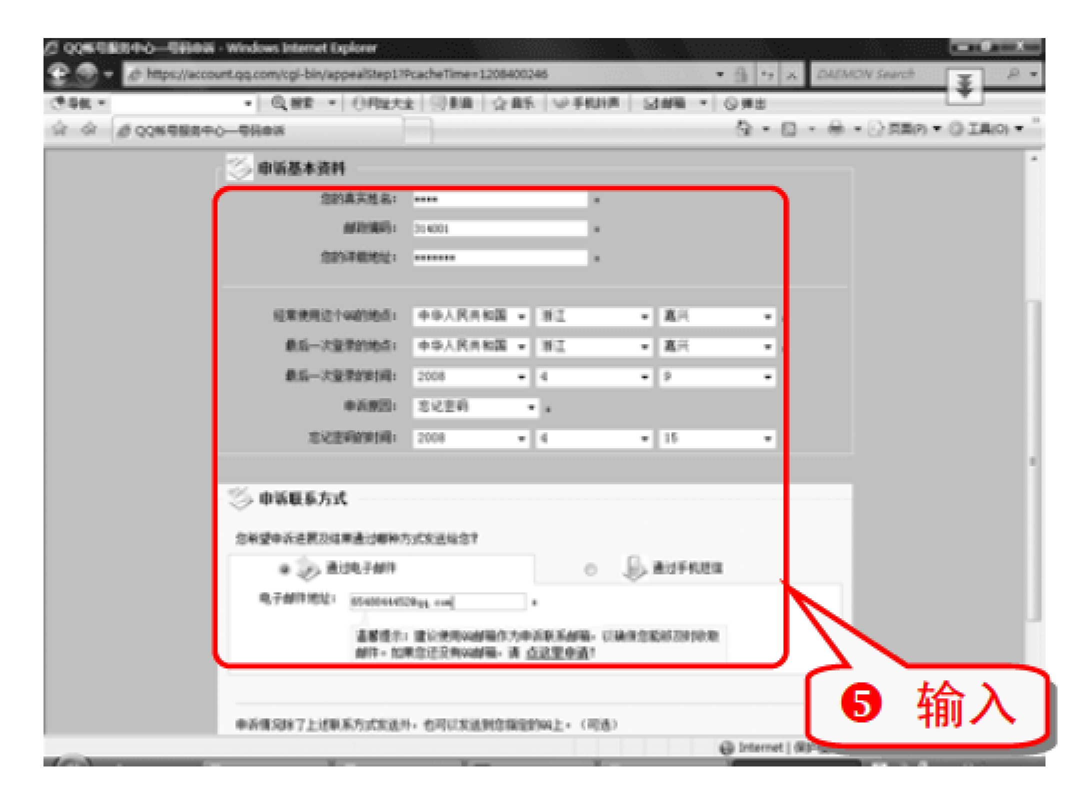
如果未申请或已忘记密码保护资料，可以通过“申诉找回密码”按钮找回密码。

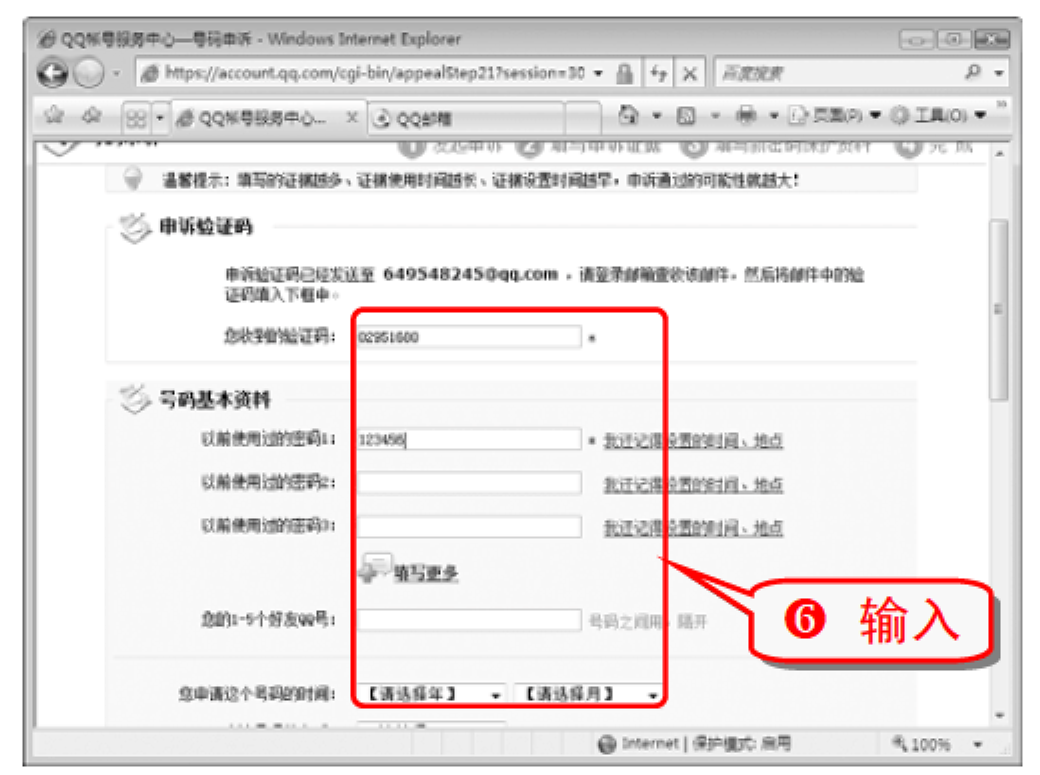
❶ 打开腾讯客户服务中心官方网站。



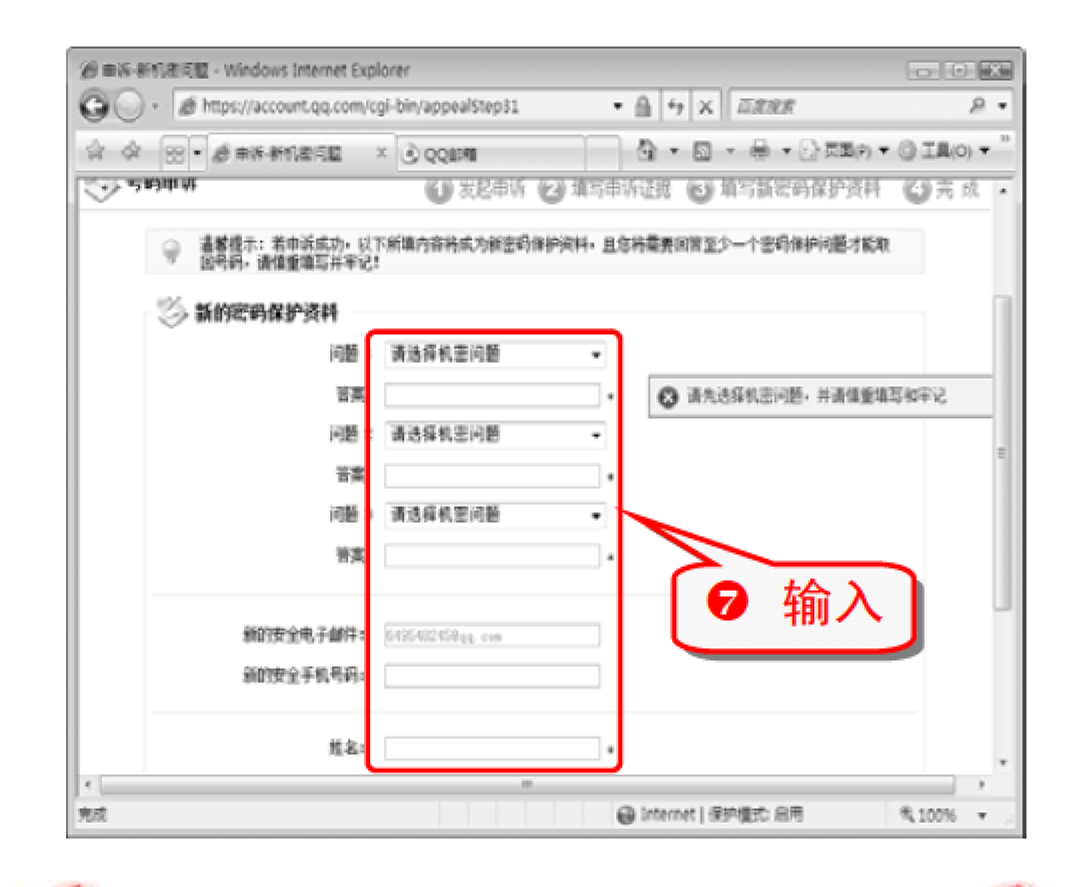












注　意　事　项

资料要填写正确和完整，并且将其记录下来，在下次找回密码的时候都要输入这些资料。

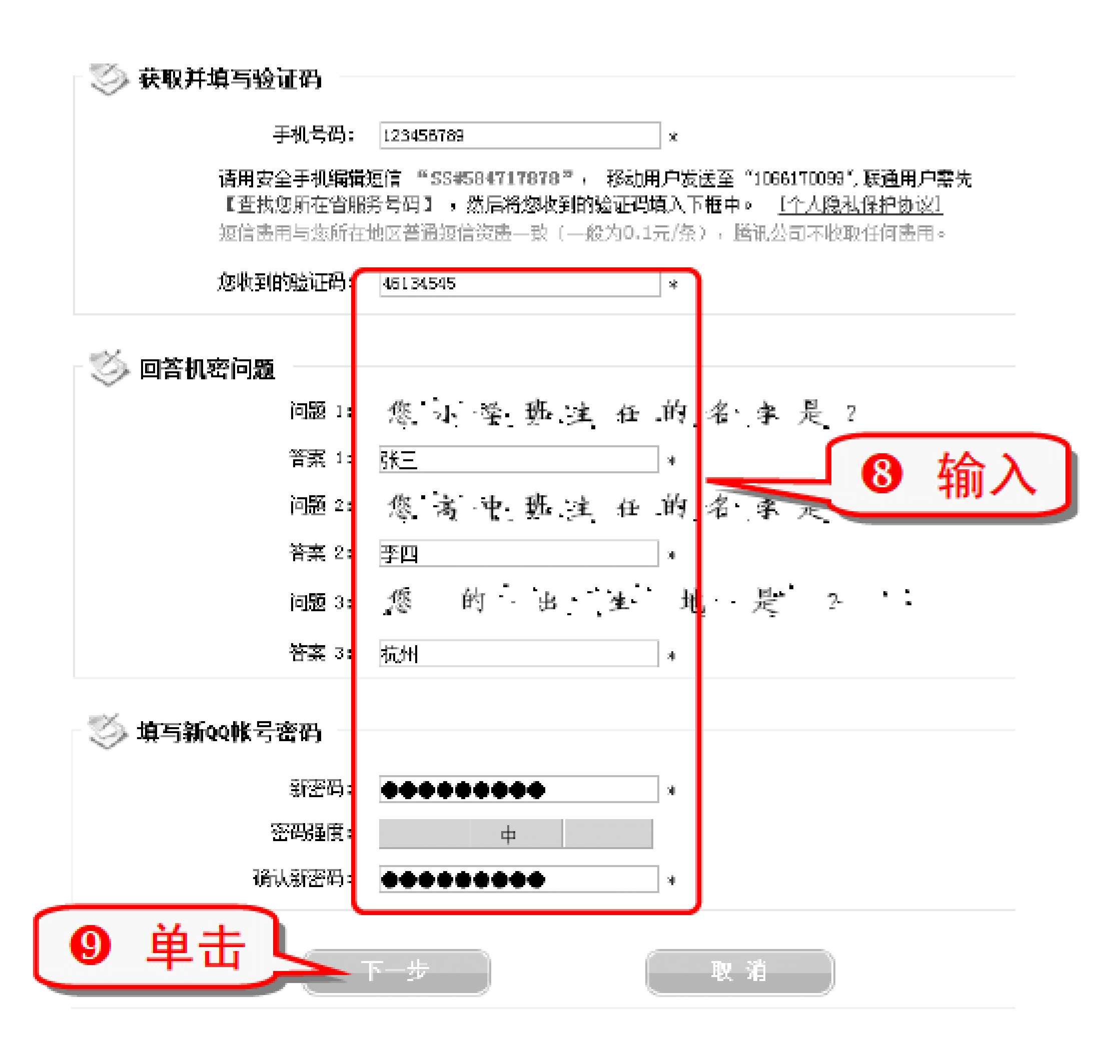
(2) 申请密码保护的情况下

如果已申请并记得密码保护资料，则可通过“自动找回密码”按钮找回密码。

❶ 打开腾讯客户服务中心官方网站，选择“密码找回”区域中的“点击进入”按钮→单击“自动找回密码”按钮。







技巧100　巧用 QQ 空间密码猜解工具破解密码

访问好友空间的时候，好友设置了访问问题，又不想去麻烦好友，可以尝试用 QQ 空间密码猜解工具来猜解空间密码。

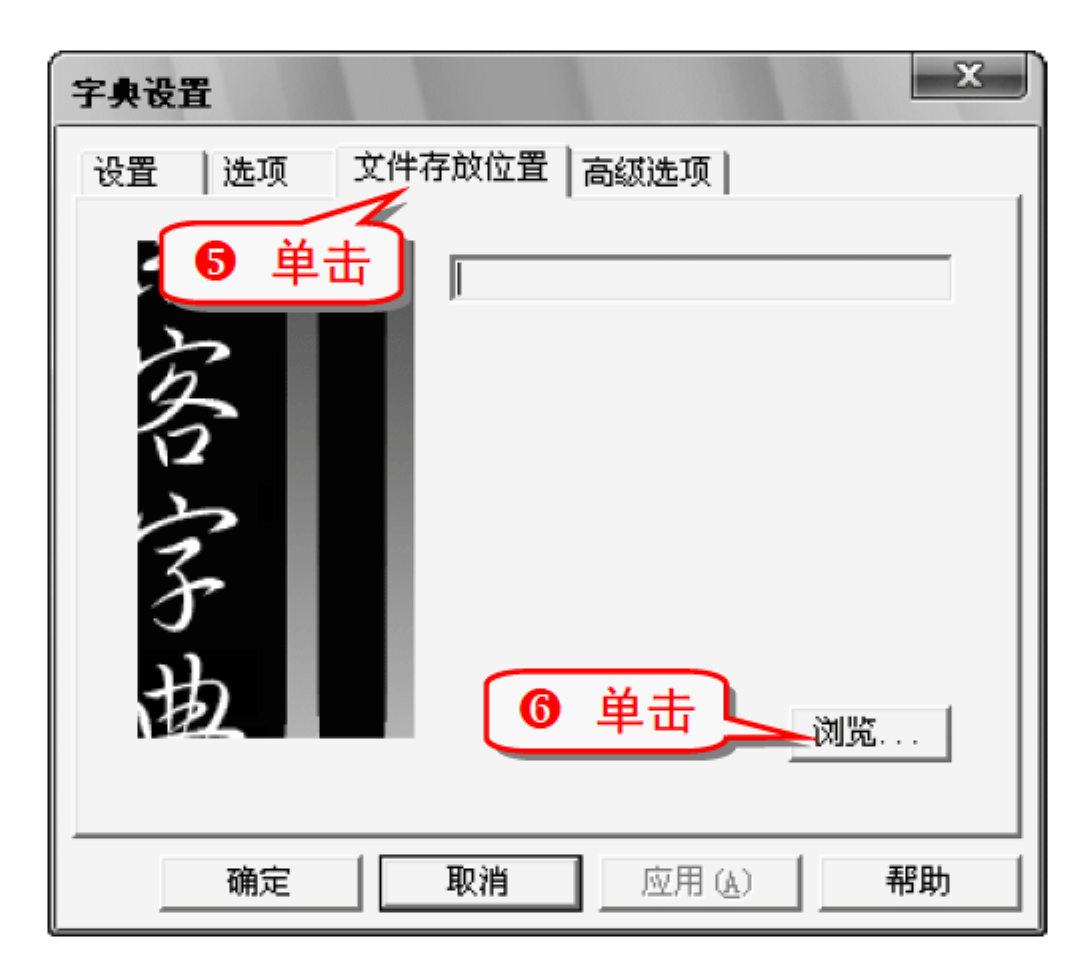
(1) 生成一个字典

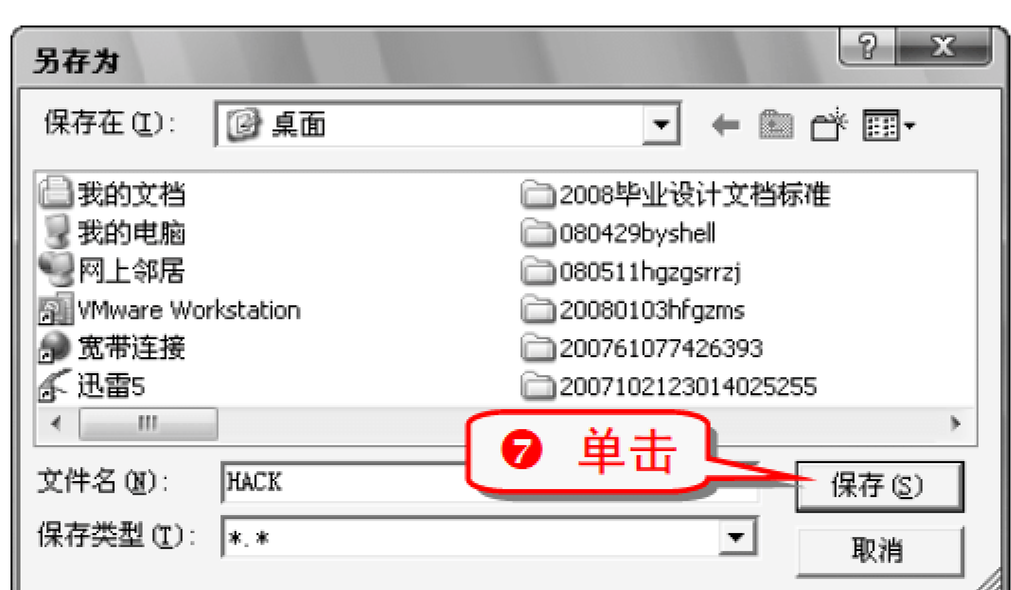
字典生成器可以根据要求，穷举出用户要求的所有组合的密码。

❶ 下载一个名为“黑客字典”的软件，双击其运行程序。







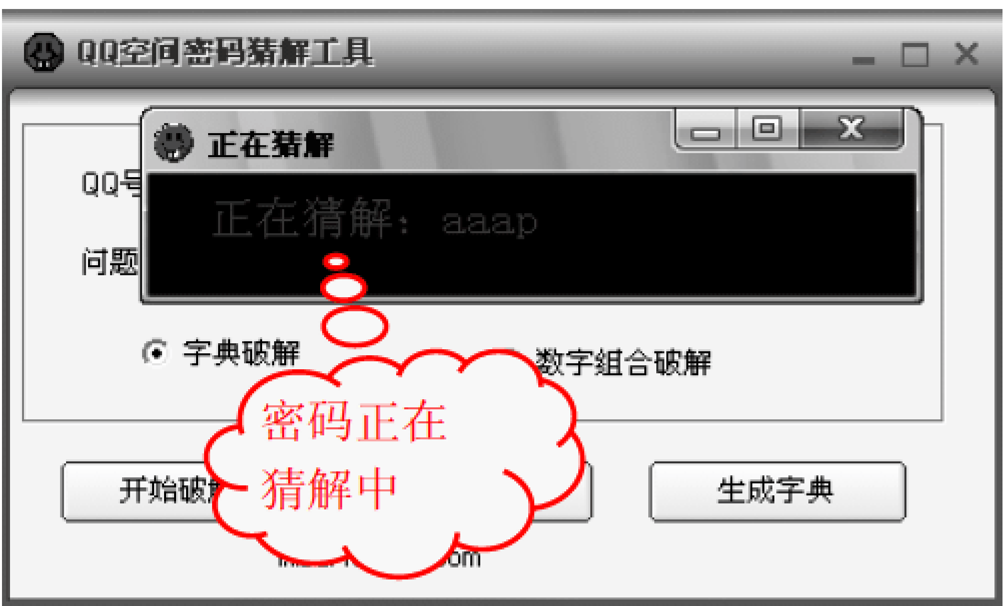


❽ 此时会在指定的目录下产生一个名为“HACK.DIC”的文件。

(2) 破解 QQ 空间密码

❶ 将生成的 HACK.DIC 的文件改名为 passtxt.txt，将其放入 QQ 空间密码猜解工具的工具包中。

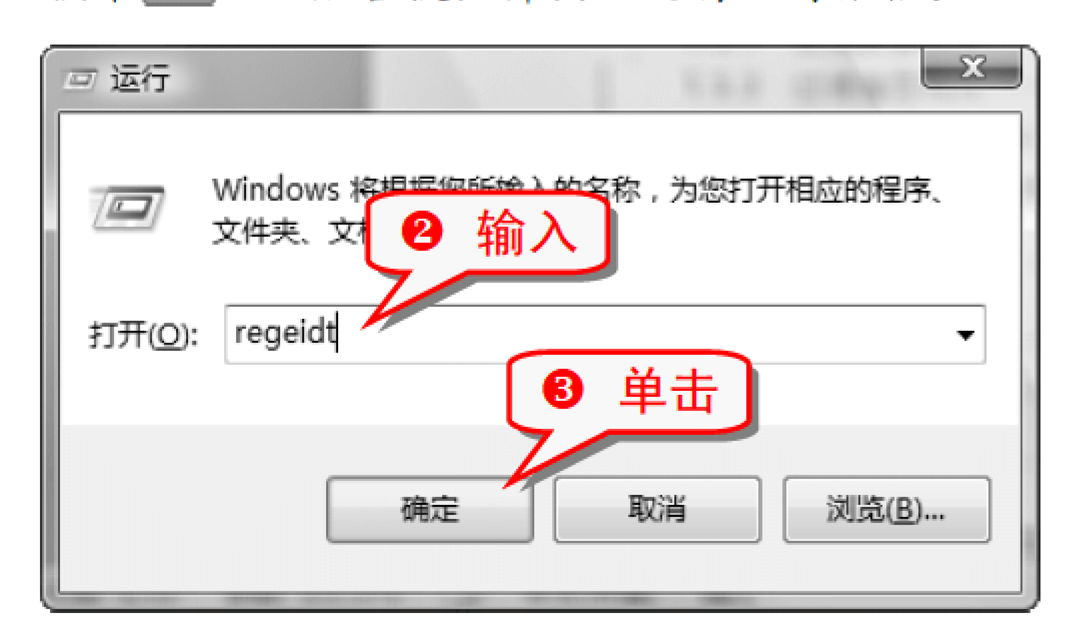




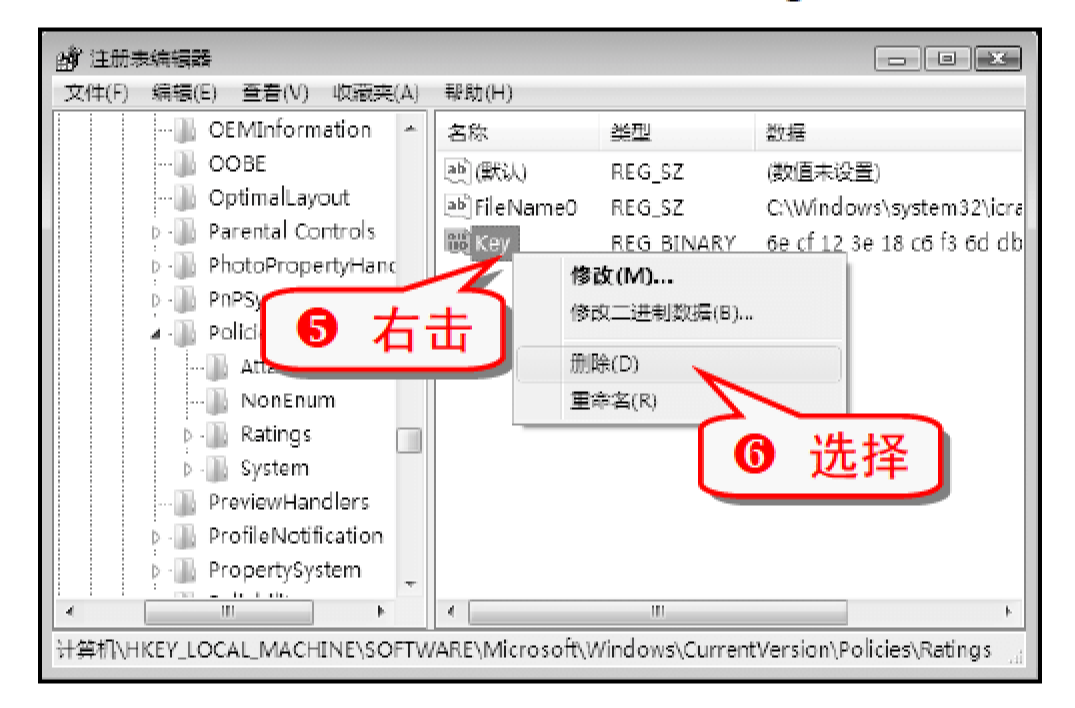
技巧101　破解 IE 内容分级审查密码

忘记 IE 内容分级审查密码会造成很多不便，通过修改注册表可以删除 IE 内容分级审查密码。

❶ 按下 ⊞ + R 组合键，弹出“运行”对话框。



❹ 展开 HKEY_LOCAL_MACHINE\SOFTWARE\Micro soft\Windows\CurrentVersion\Policies\Ratings 分支。



技巧102　利用系统自带工具制作密码重置盘

Windows Vista 系统中具有密码重置的功能，用户利用 U 盘做一个密码重置盘，用 U 盘就能对登录密码进行重置。

(1) 制作密码重置盘

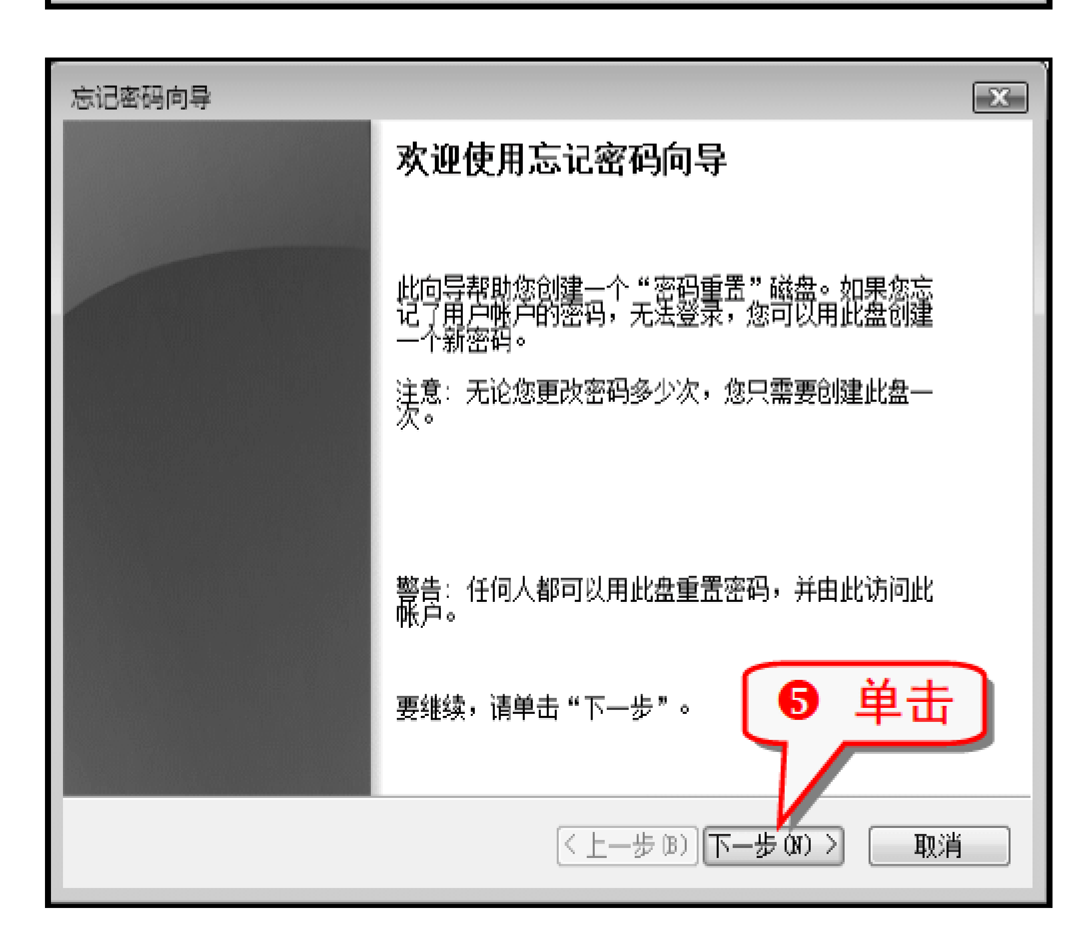
❶ 进入 Windows Vista 系统，插入打算作为密码重置盘的 U 盘，选择“开始”→“控制面板”命令。

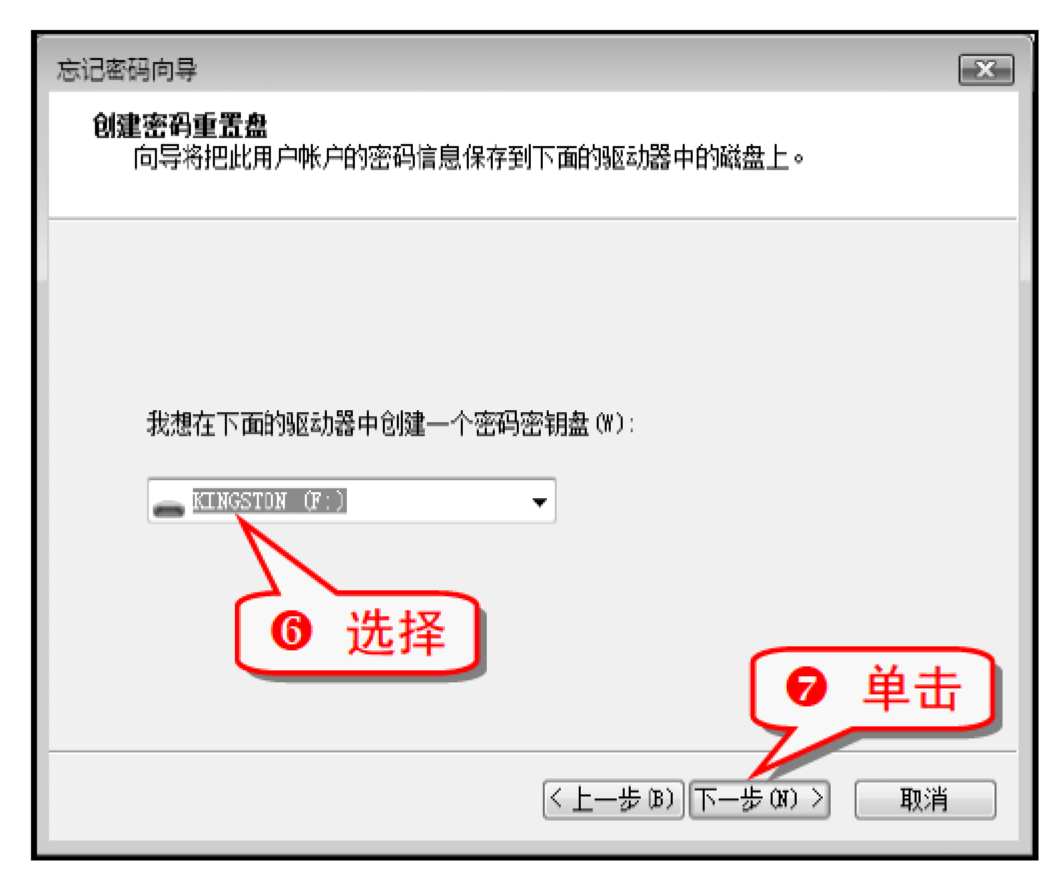


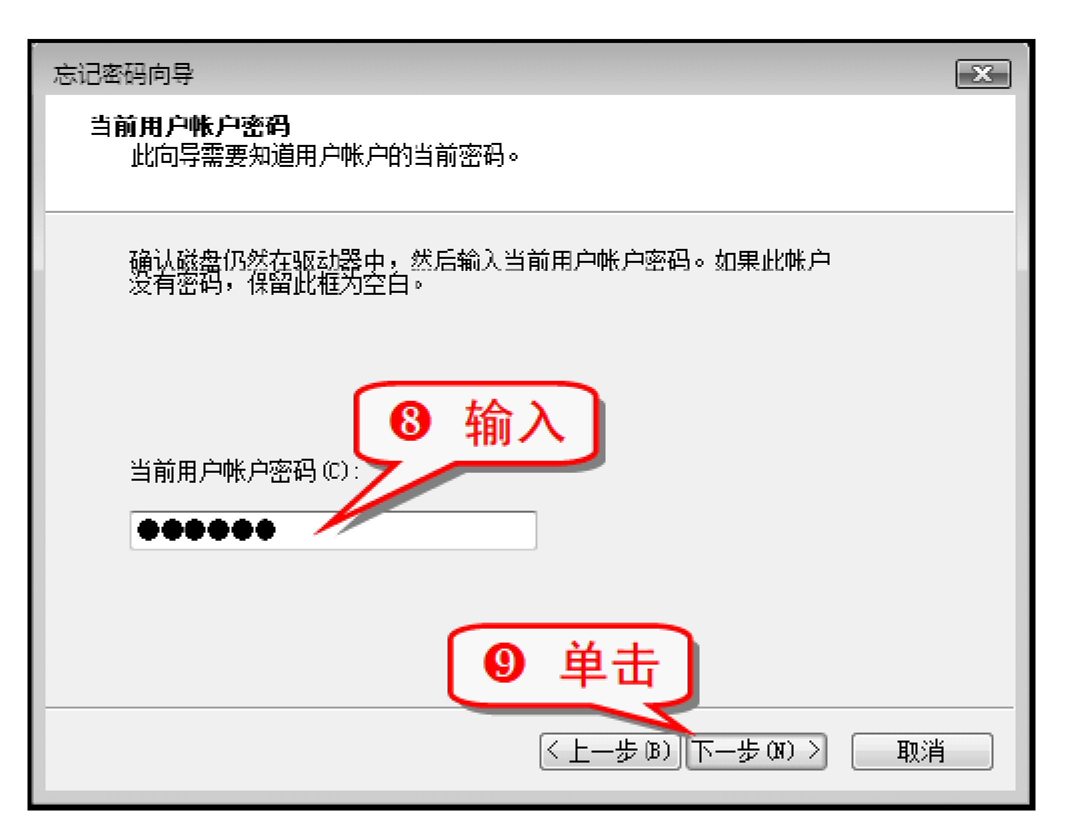


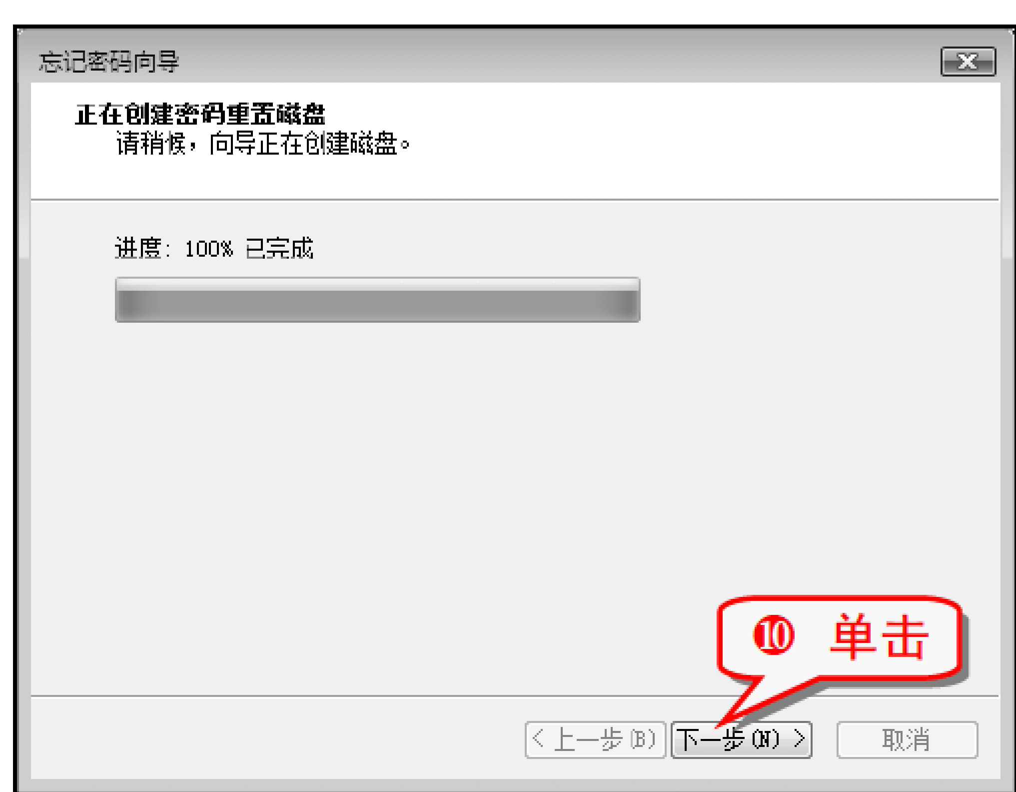










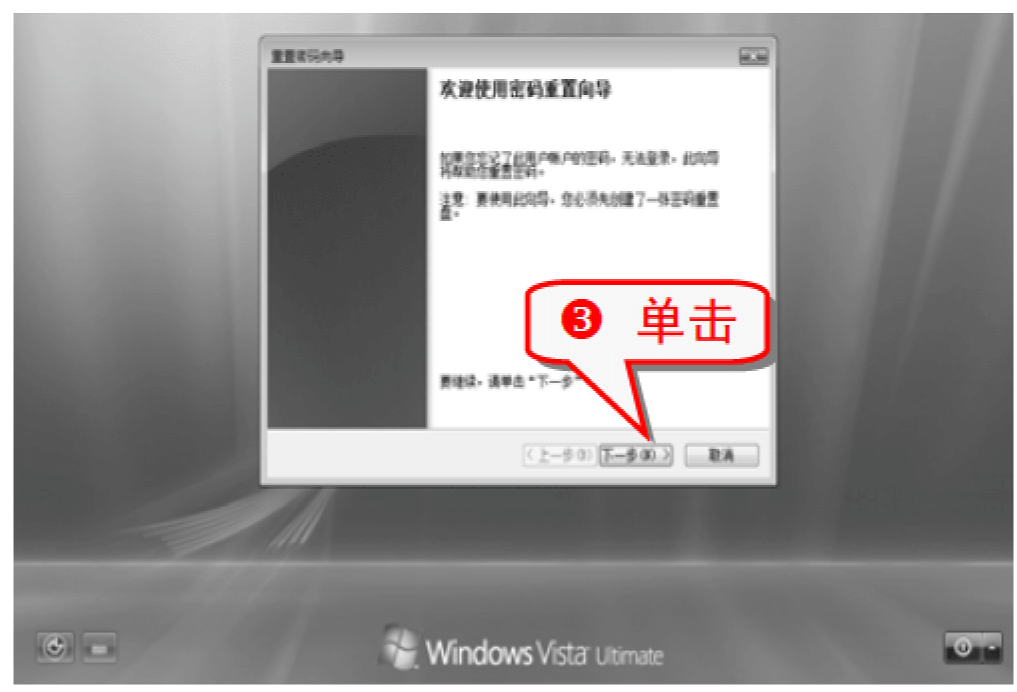


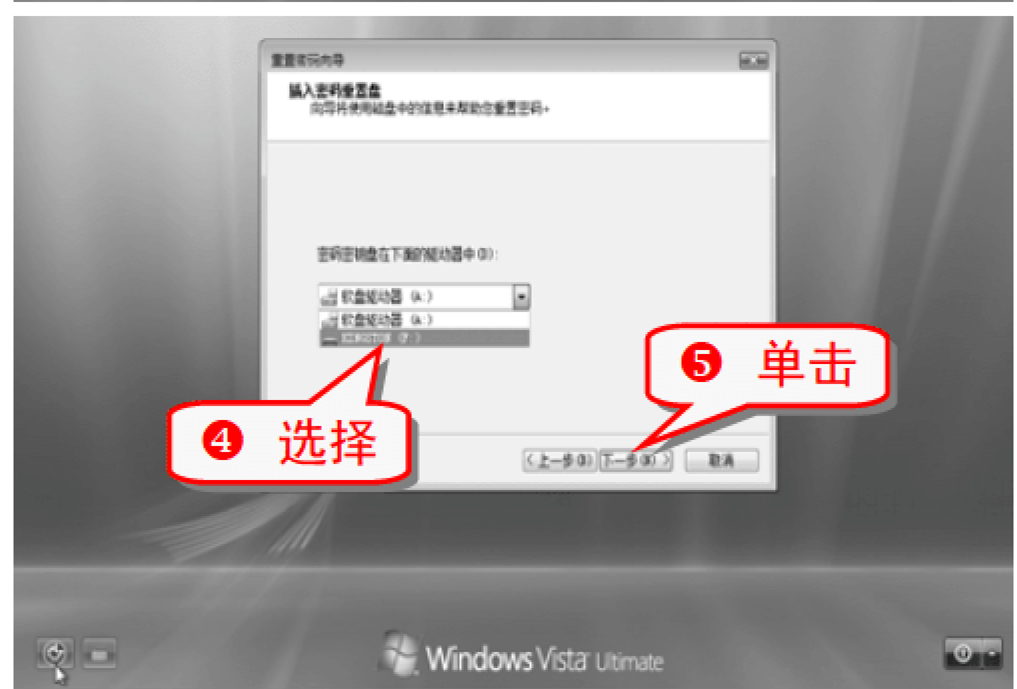


(2) 进行密码重置

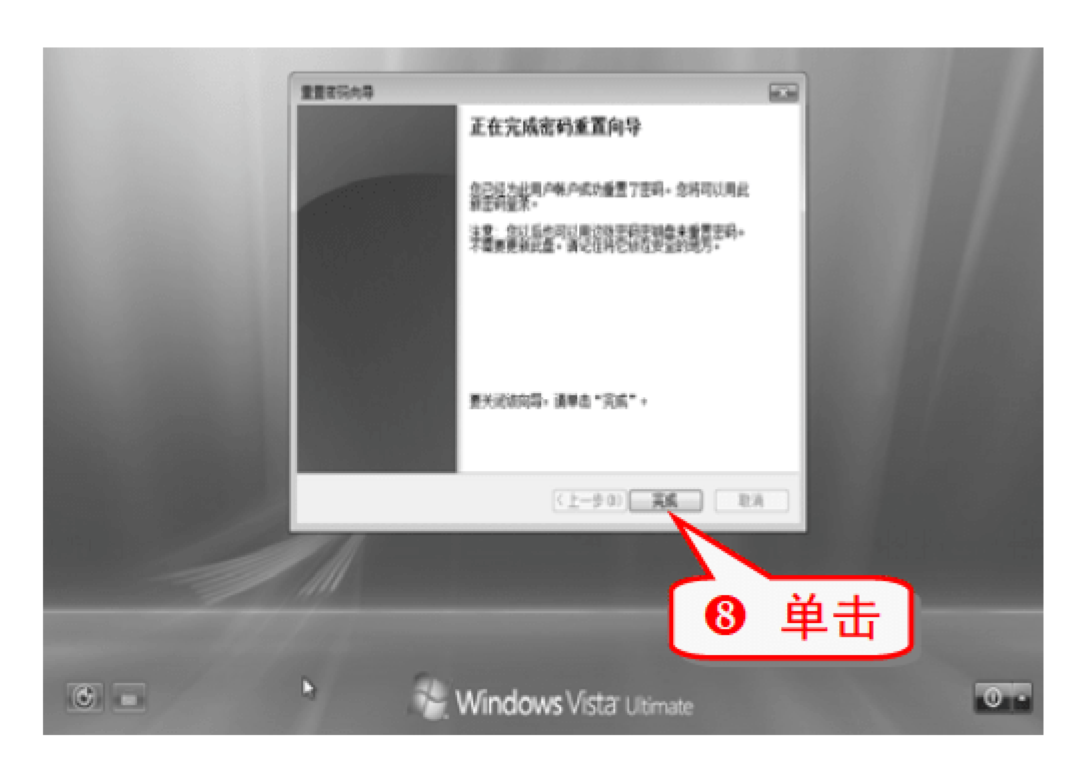
❶ 启动电脑，进入登录界面，插入作为密码重置盘的U盘。











注 意 事 项

密码重置盘很重要，有了这个U盘就可以轻松地进入Windows Vista系统。所以U盘要妥善保管。而且无论更改过多少次登录密码，只要拥有这个U盘就可以进行密码重置。



专 家 坐 堂

用户只能有一个有效的密码重置盘，而且只有最近一次制作的盘有效，之前所有密码重置盘都会在新盘生成时失效。针对于其中一个Windows Vista系统创建的userkey.psw文件无法在另一个Windows Vista系统中实现密码重置功能，即使两台电脑系统中的用户名和密码都是一样的。

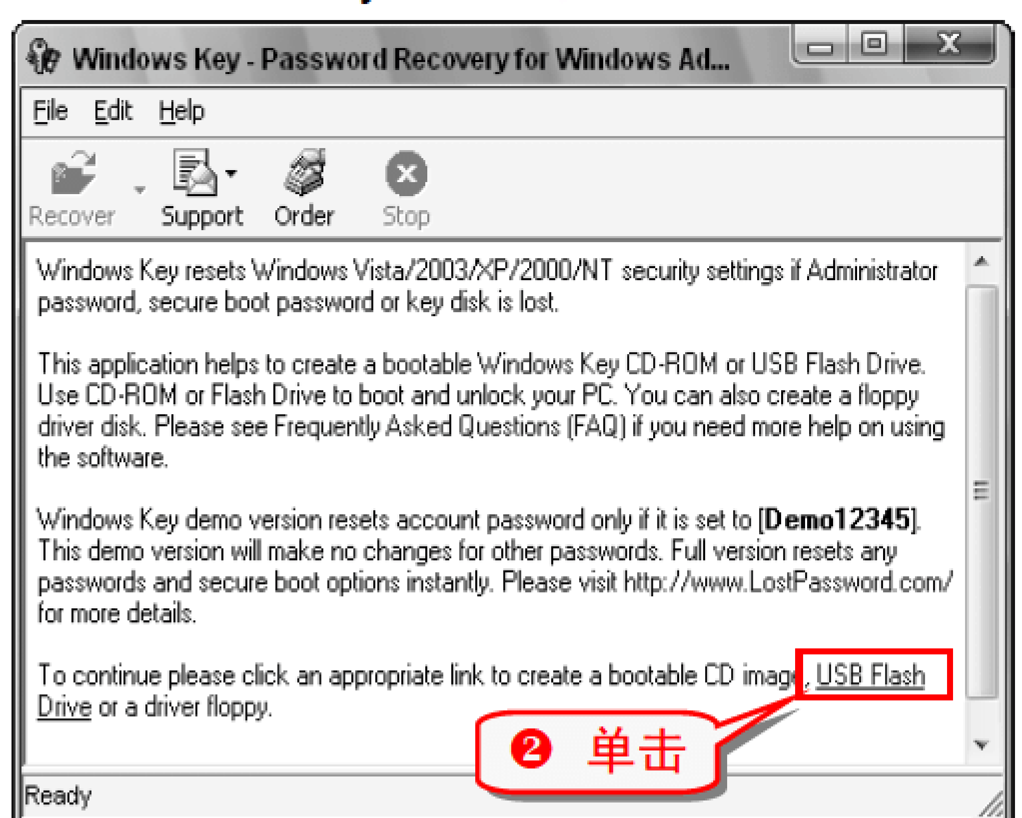
技巧103 巧用 Windows Key 制作密码重置盘

Windows Key能够恢复被遗忘的用户登录密码，使用Windows Key创建一个启动密钥盘，可以让用户不再因登录密码的丢失而发愁。

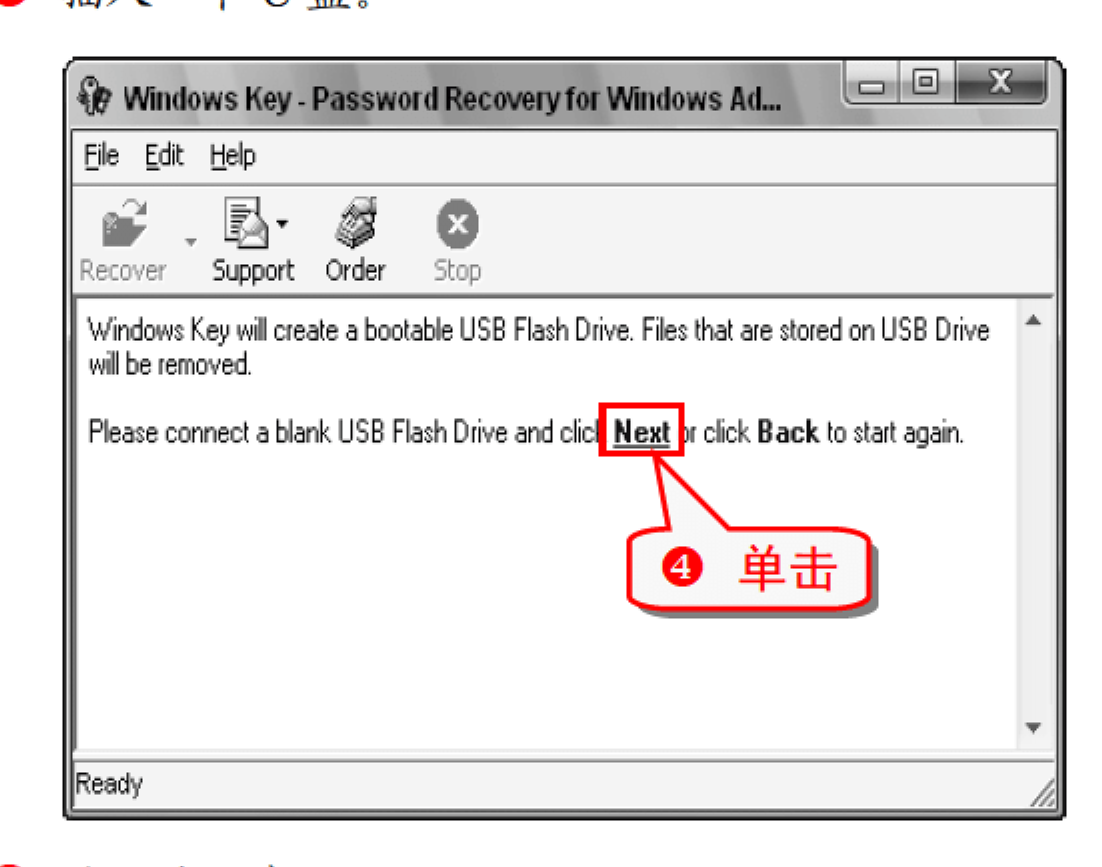
(1) 创建启动密钥盘

创建启动密钥盘需要的工具有：一张系统安装光盘和一个U盘。

❶ 运行Windows Key启动程序。

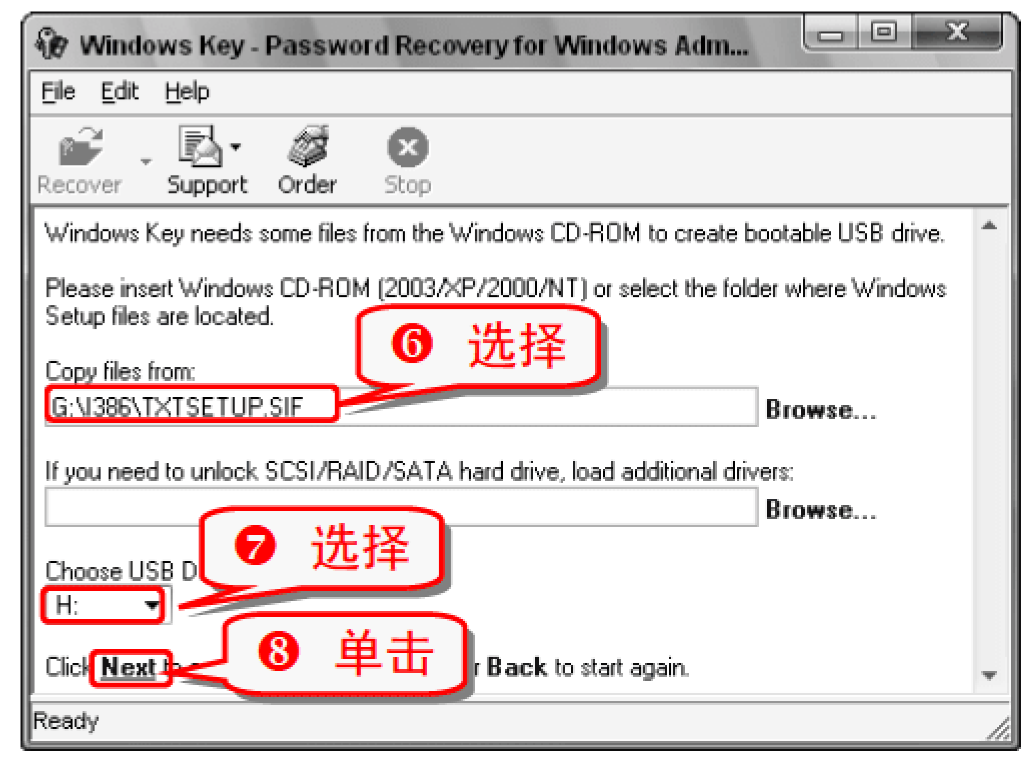


❸ 插入一个U盘。



❺ 放入系统盘。







❾ 提示创建完成后，单击“确定”按钮。

(2) 使用启动密钥盘

❶ 插入系统安装盘，重新启动电脑。

❷ 当界面上出现 Press F6 if you need install party SCSI or RAID driver…时，按下 F6 键。

❸ 在加载结束后立即按下 S 键。

❹ 插入 U 盘，按下 Enter 键。

❺ 系统进入 Windows Key 环境，提示：“Set Adminstrator Password to ‘123456’? (Y/N)”，此时输入 Y，并按下 Enter 键，密码重置成功。



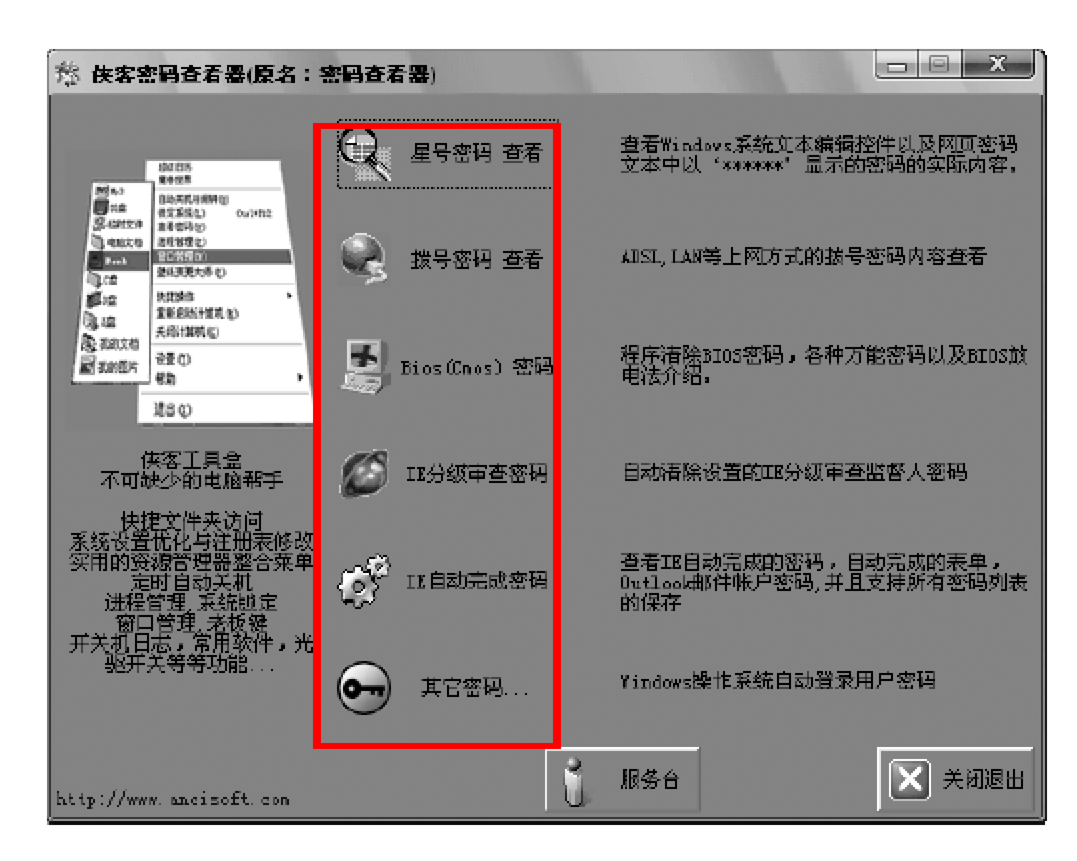
只能使用“123456”作为重置密码。

技巧104　巧用侠客密码查看器

侠客密码查看器是一款功能丰富的密码查看器，有如下功能。

- 查看 Windows 系统中显示的星号密码。
- 支持 ADSL 和 LAN 上网密码的查看。
- 查看网页中显示的星号密码。
- 支持 IE 自动完成的密码、表单内容查看与密码列表保存。
- 查看 Windows 自动登录密码。
- 支持 CMOS 开机密码的清除。
- 支持 IE 分级审查密码的清除。

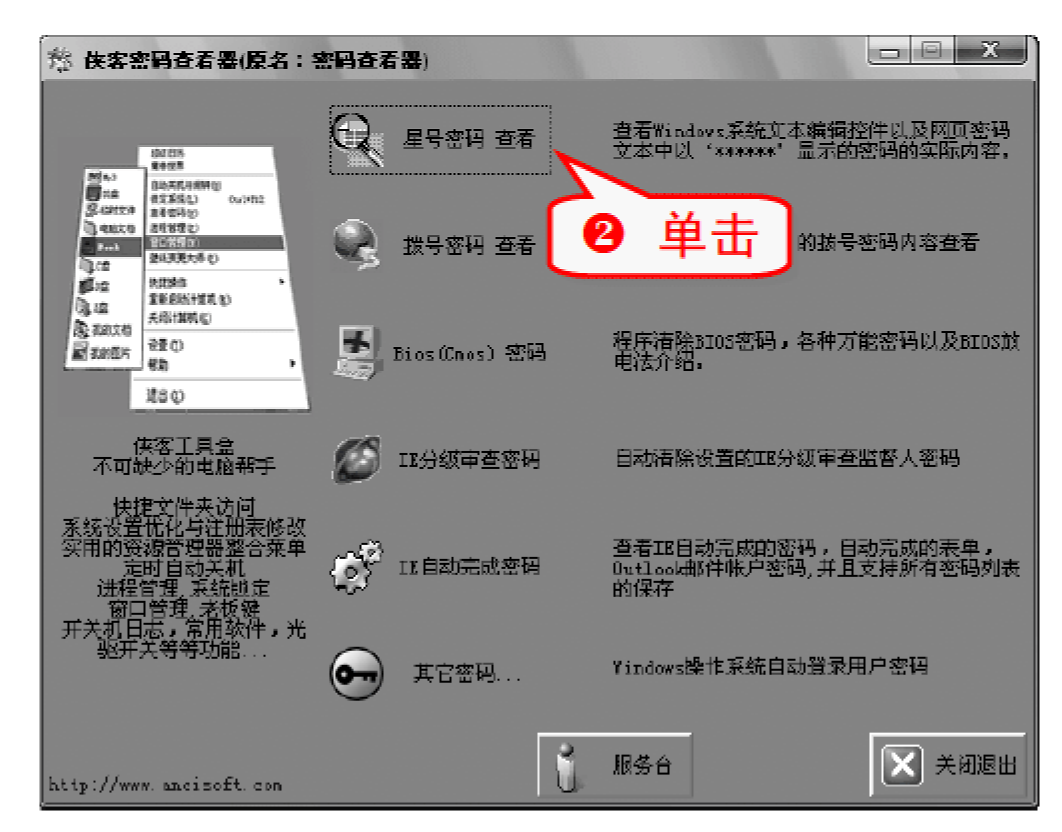
其主界面如下图所示，提供 5 个功能按钮。



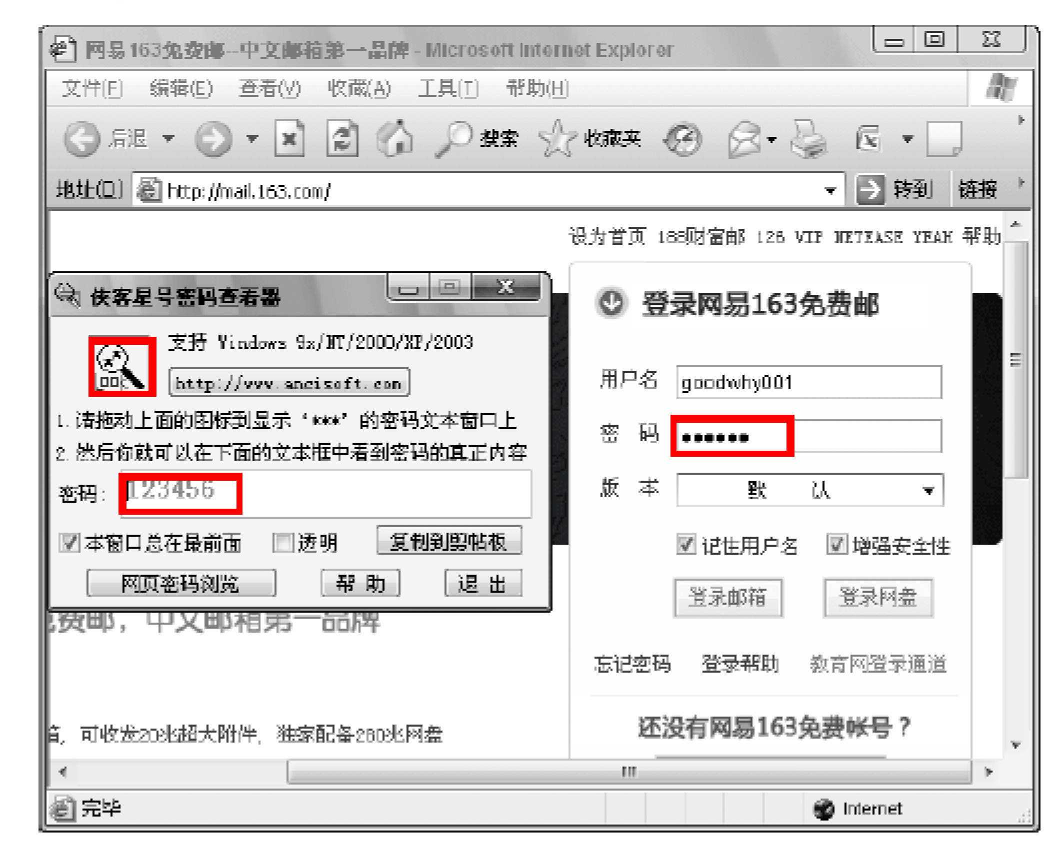
(1) 星号密码查看

利用软件可以快速查看 Windows 各种版本系统“***”密码的真正内容，也可以查看 IE 网页浏览器里显示的“***”密码的真正内容。

❶ 打开“侠客密码查看器”主窗口。



❸ 拖动密码查看器窗口中的放大镜图标到显示的密码上面。

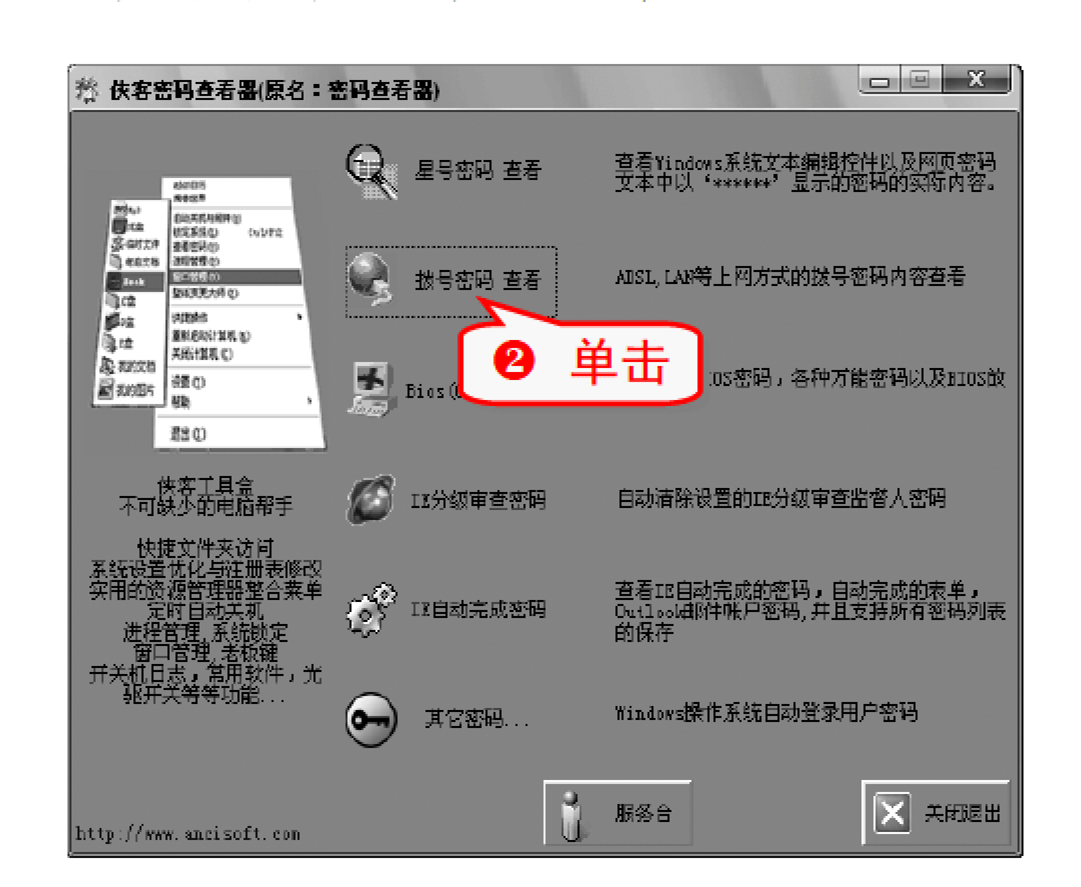


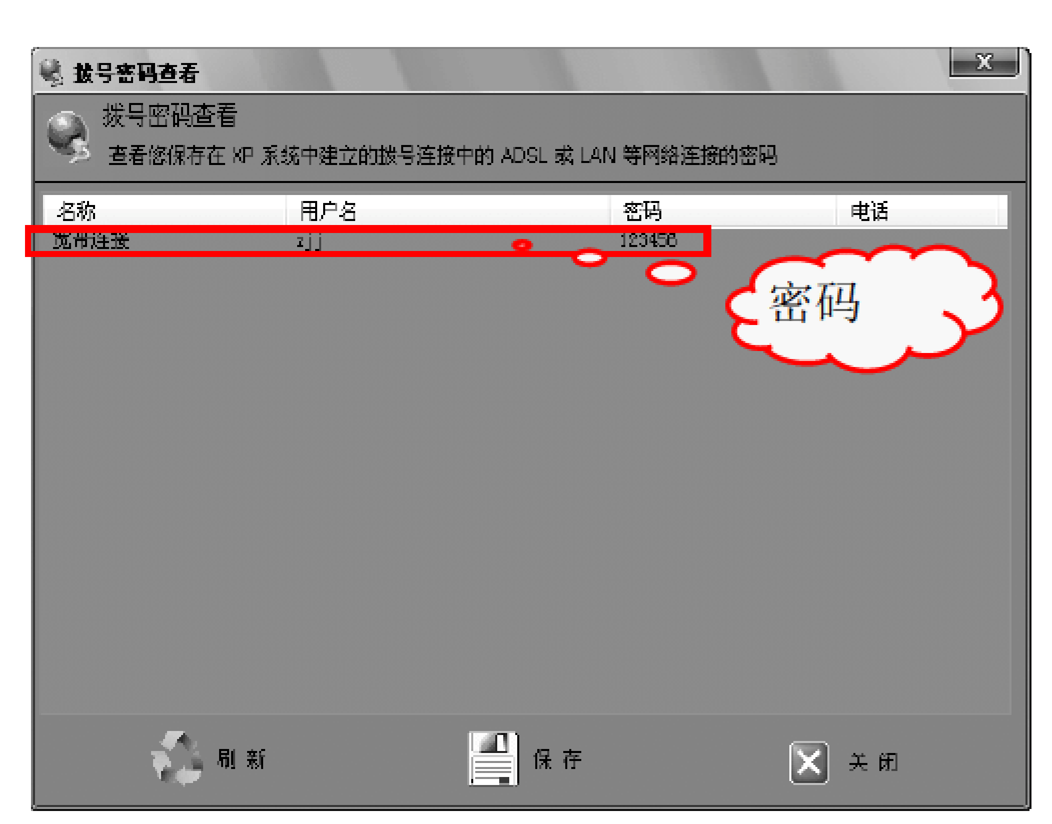
(2) 拨号密码查看

利用软件查看 Windows XP 系统中建立的网络连接

(包括 ADSL 上网连接和 LAN 上网连接)中所保存的用户名和密码。

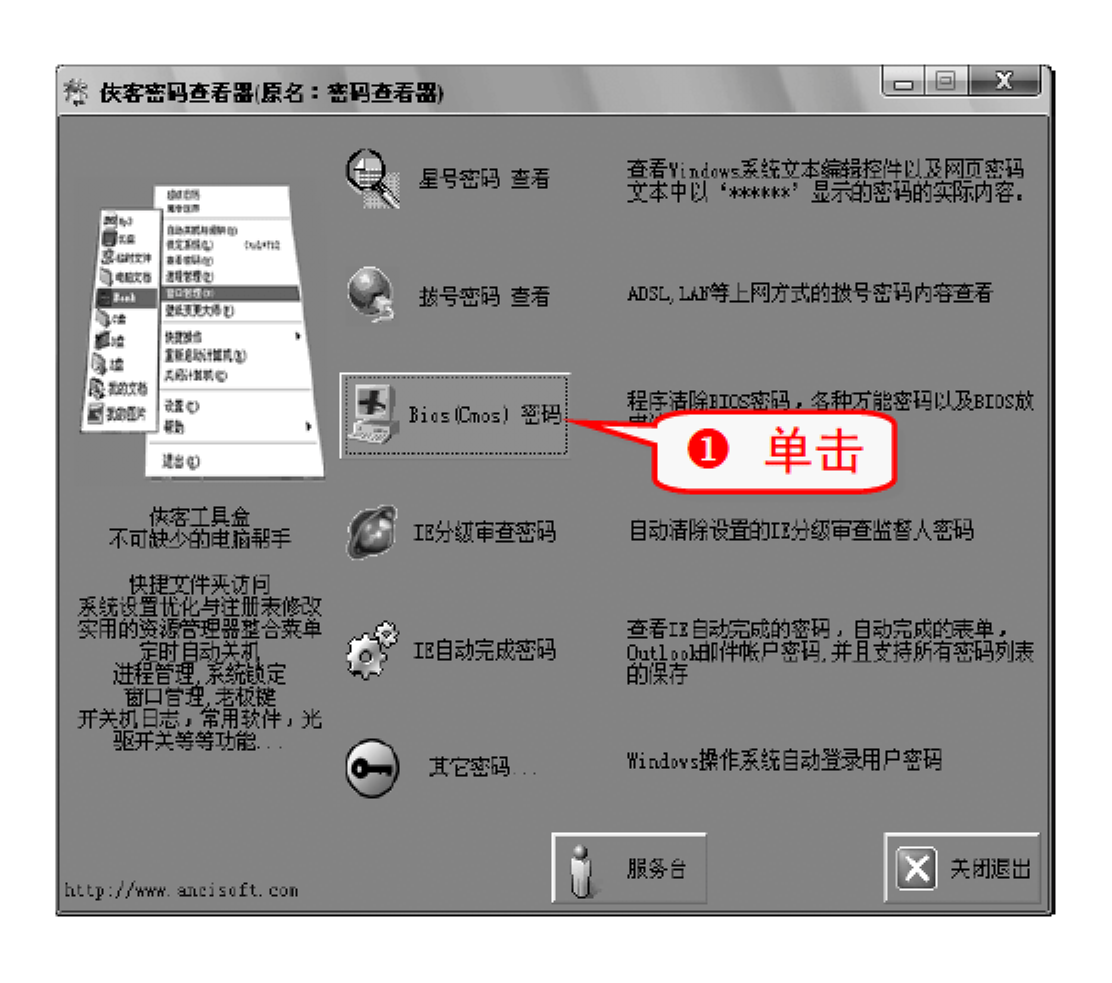
❶ 打开“侠客密码查看器”主窗口。

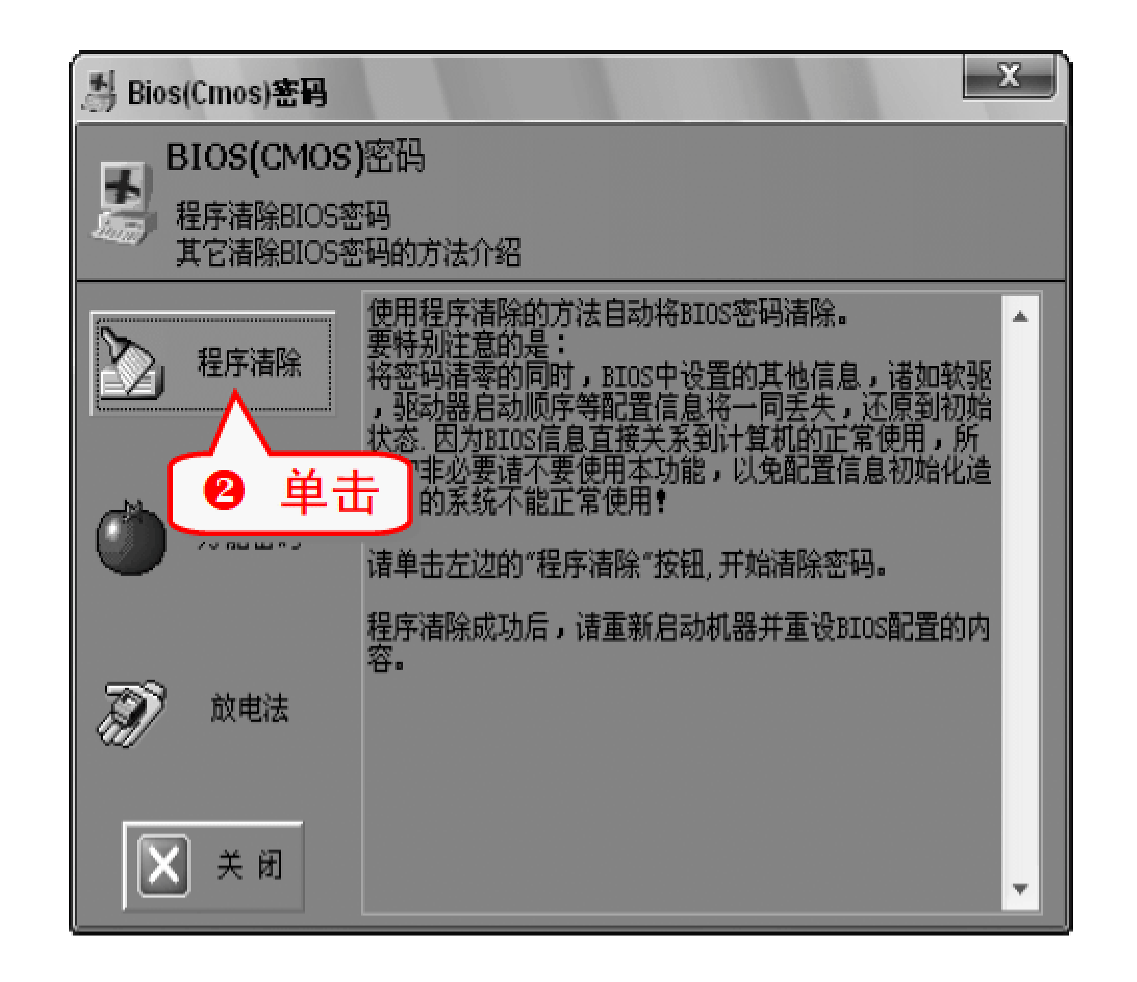




(3) 清除 BIOS 密码

利用软件快速清除 BIOS 密码，无需进入 BIOS 进行设置。

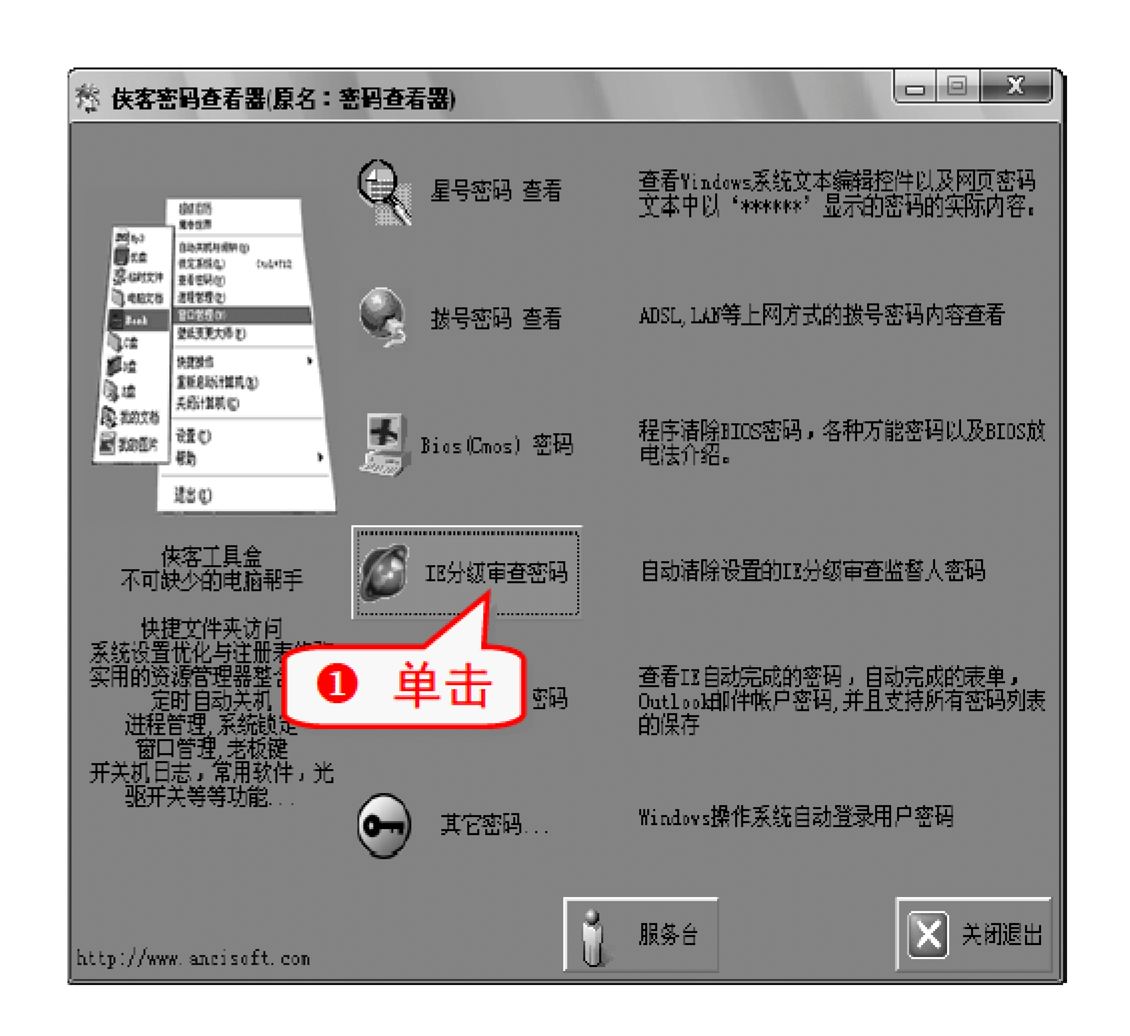




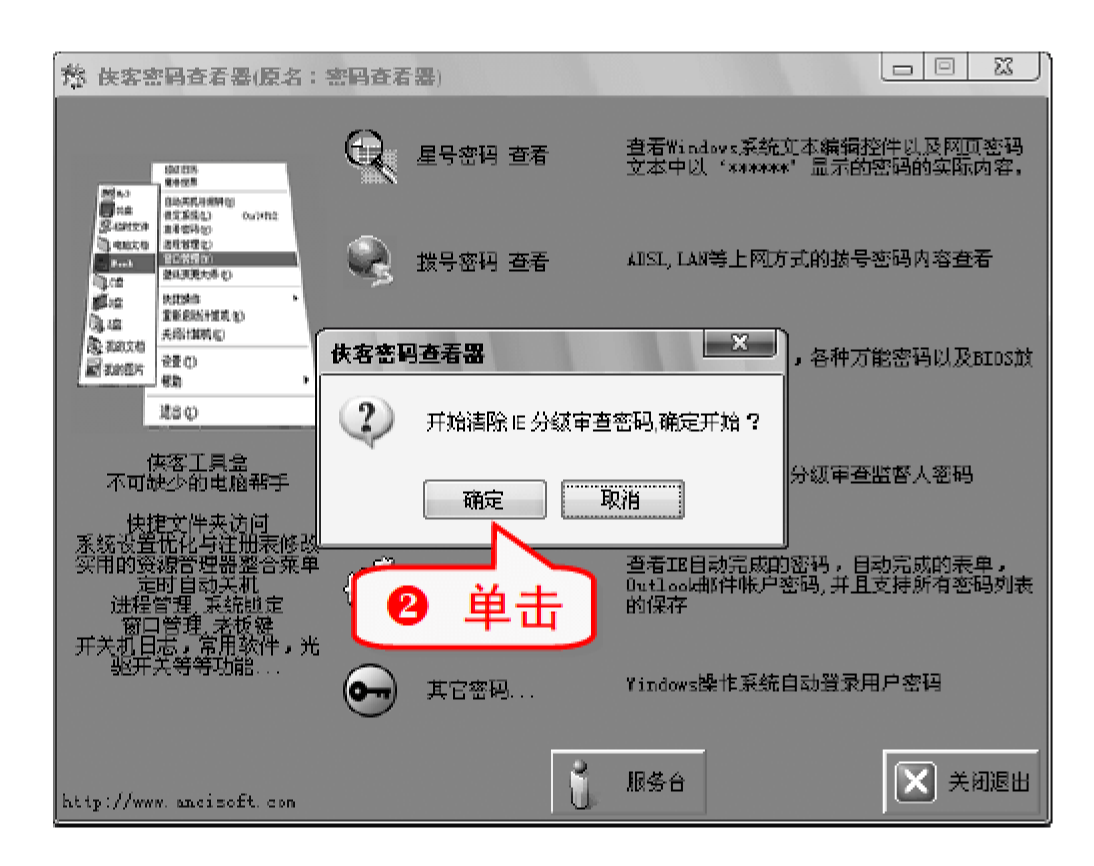


(4) 清除 IE 分级审查密码

利用软件快速清除 IE 分级审查密码，无需借助注册表。



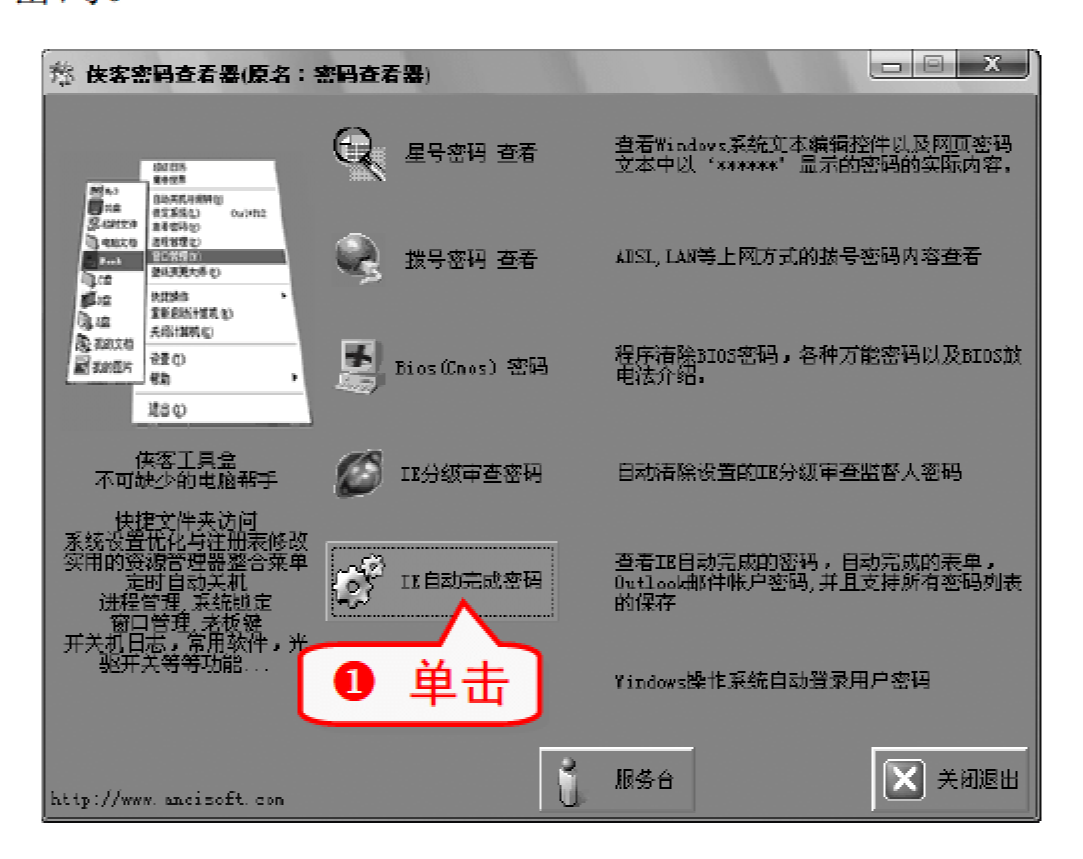


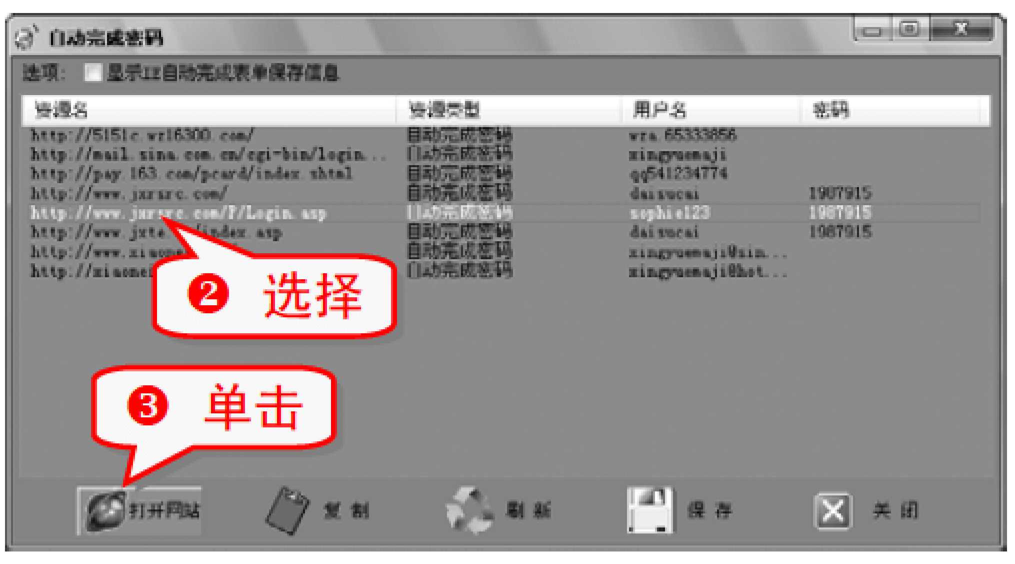




(5) IE 自动完成密码

查看 IE 自动完成的表单、密码以及 Outlook 邮件账户密码。











专题五　电脑系统安全防护

内容导航

电脑的不安全因素大多都是由于人为设置不当产生的。学会对账号系统权限进行安全设置，做好系统自身的安全防护，可以很好地提高系统的安全系数。

热点快报

- 伪装陷阱账户技巧
- 禁用注册表
- 禁用可移动磁盘
- 禁用来宾账户
- 禁用自动播放功能
- 设置家长控制

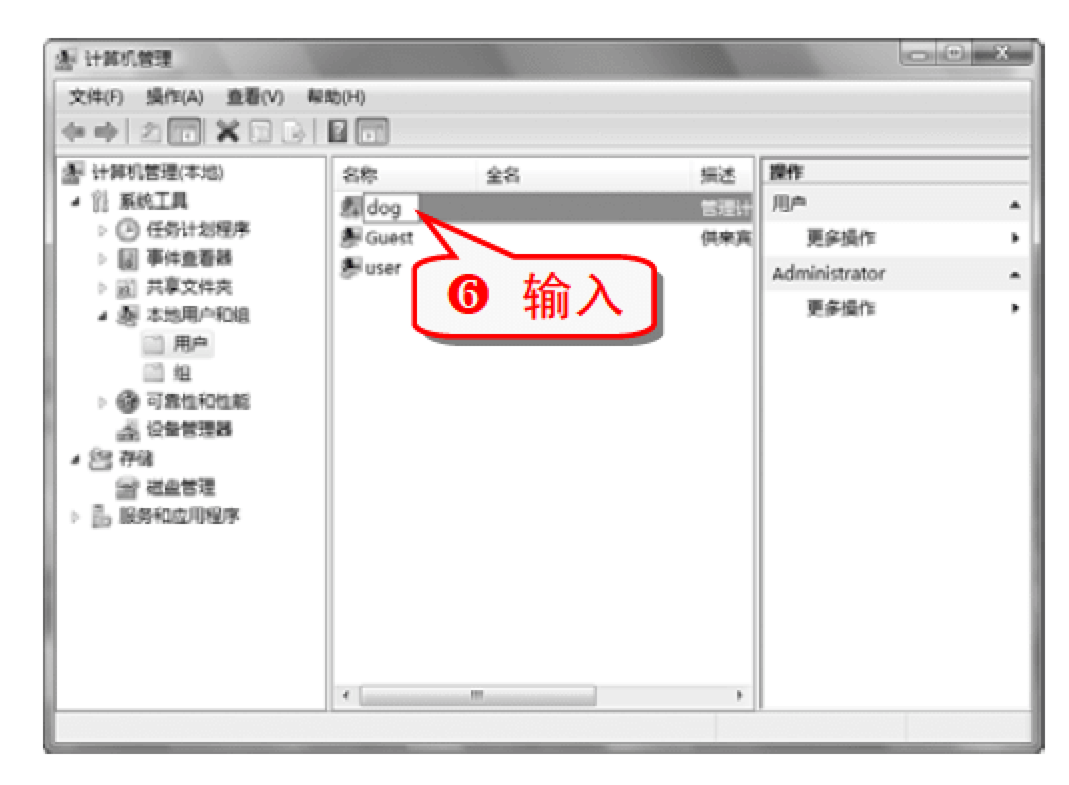
技巧105　更改系统管理员账户名

Administrator 账户是系统安装后的默认系统管理员账户，具有对系统进行一切管理的权限。针对 Administrator 账户存在的潜在危险，可以通过更改账户名的方式进行伪装以降低遭受攻击的可能性。

❶ 选择“开始”→“控制面板”→“管理工具”命令，打开“管理工具”窗口。









注 意 事 项

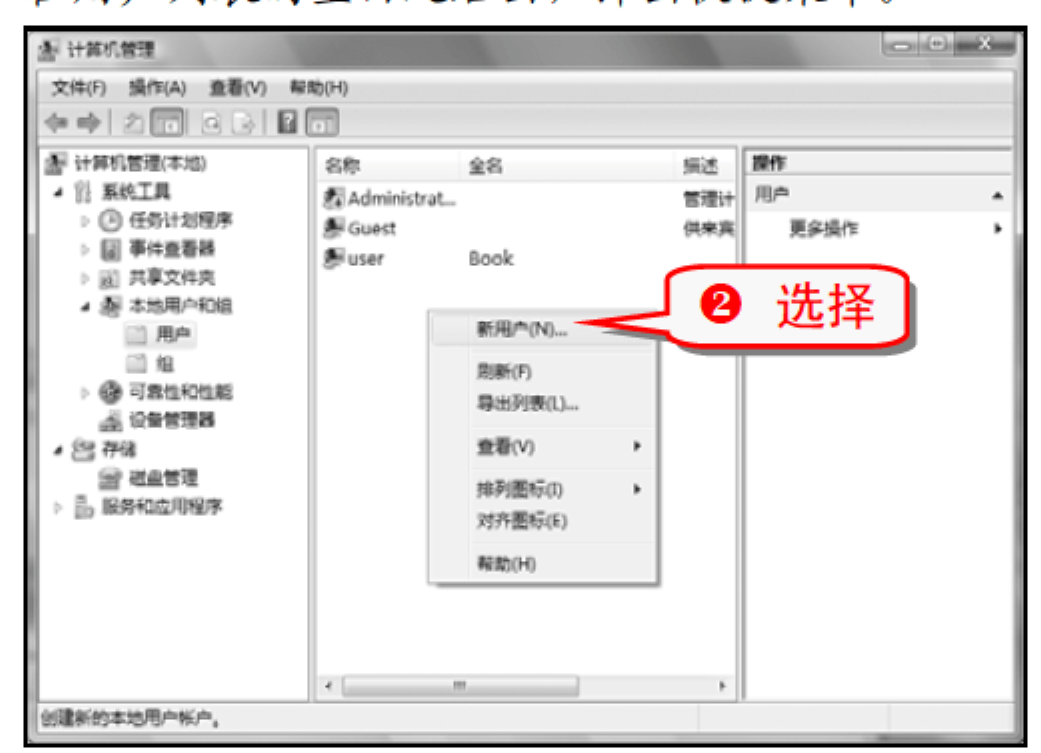
改名的时候，尽量不要将系统管理员账户名改为Admin、root等不易伪装的名字。

技巧106 为黑客伪装陷阱账户

比更改账户名更胜一筹的方法就是另建一个"Administrator"的陷阱账户，赋予其普通权限，加上一个名为复杂的密码，并对该账户启用审核。

(1) 创建新帐户

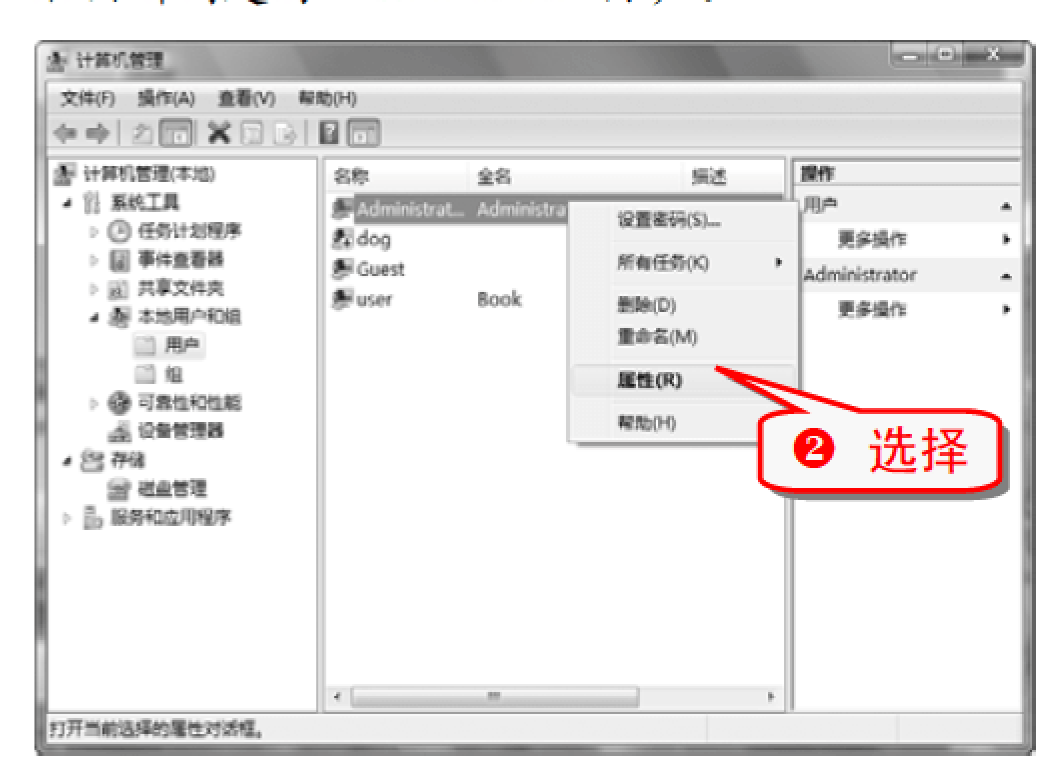
❶ 在用户列表的空白处右击，弹出快捷菜单。





(2) 添加账户权限

❶ 右击新创建的Administrator账户。







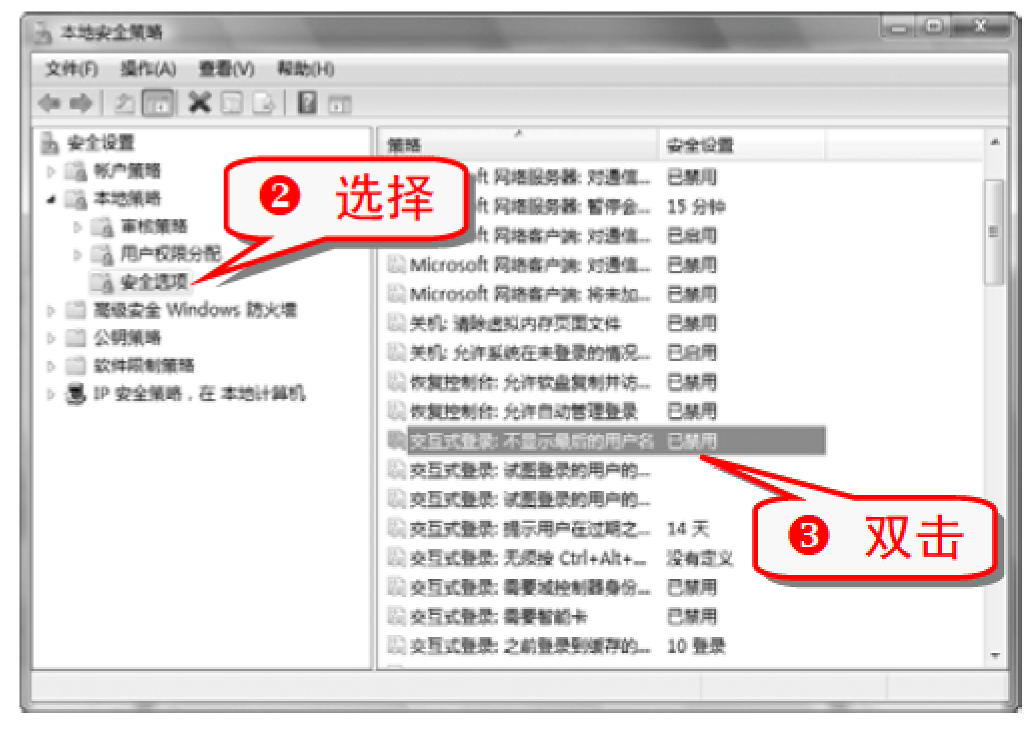


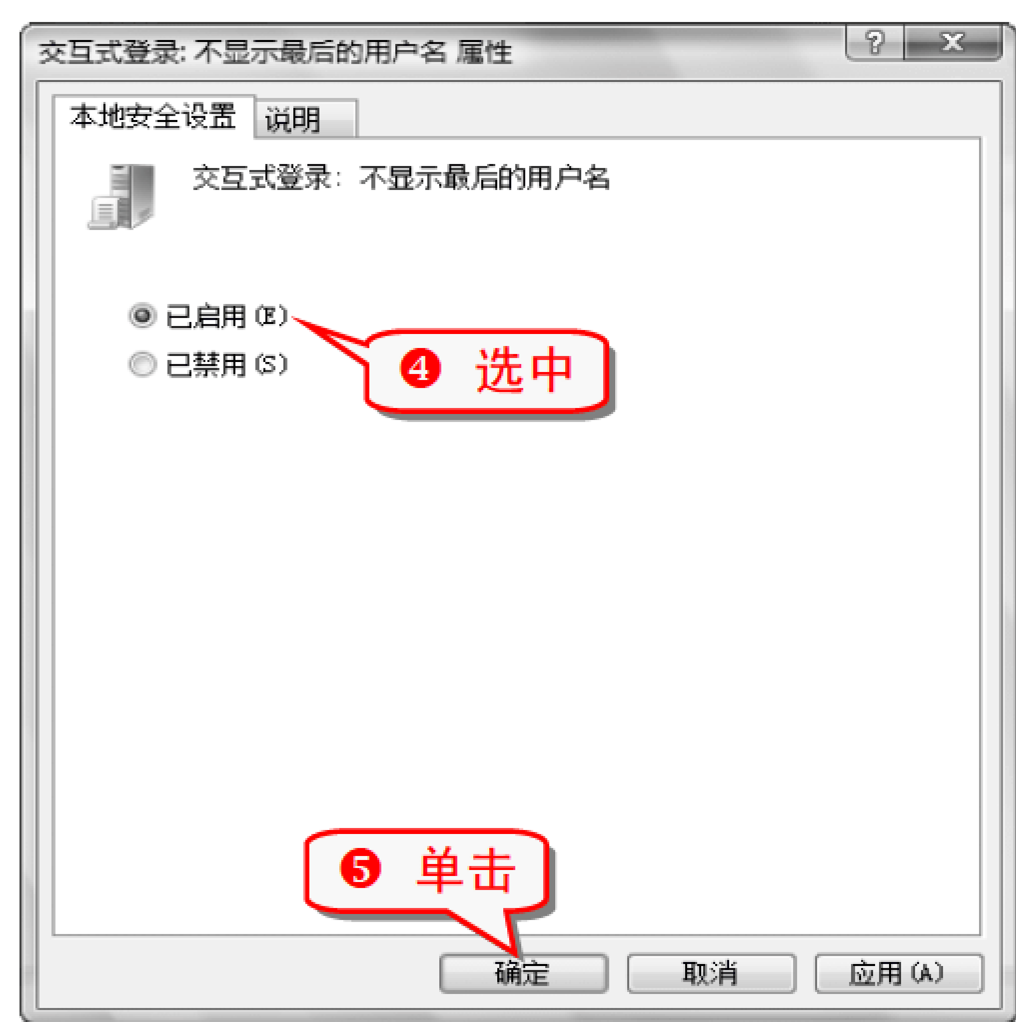




(3) 禁止显示登录用户名

❶ 选择“开始”→“控制面板”→“管理工具”→“本地安全策略”命令，打开“本地安全策略”窗口。

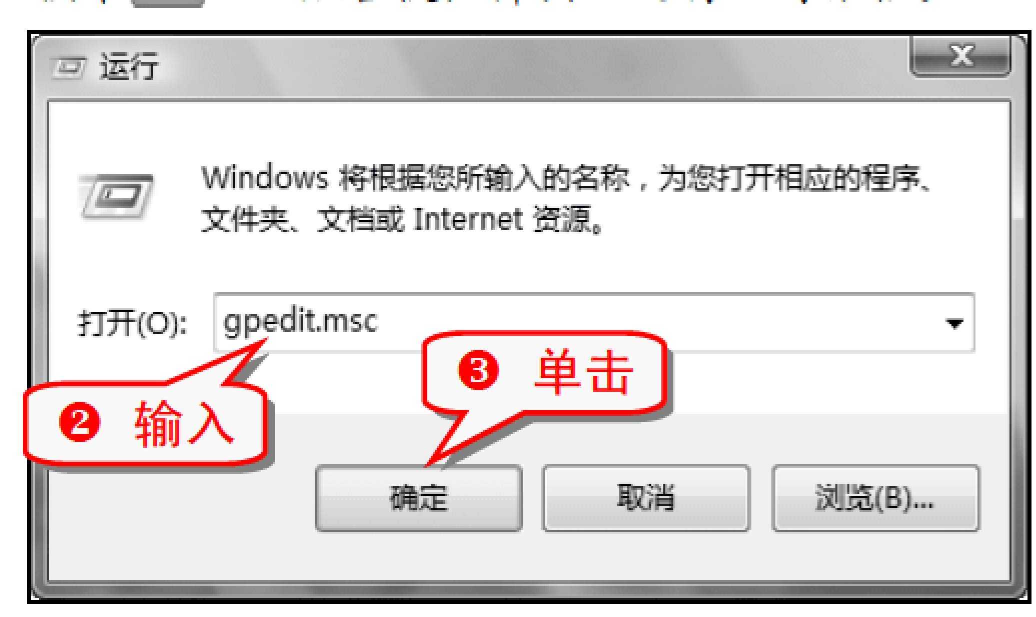




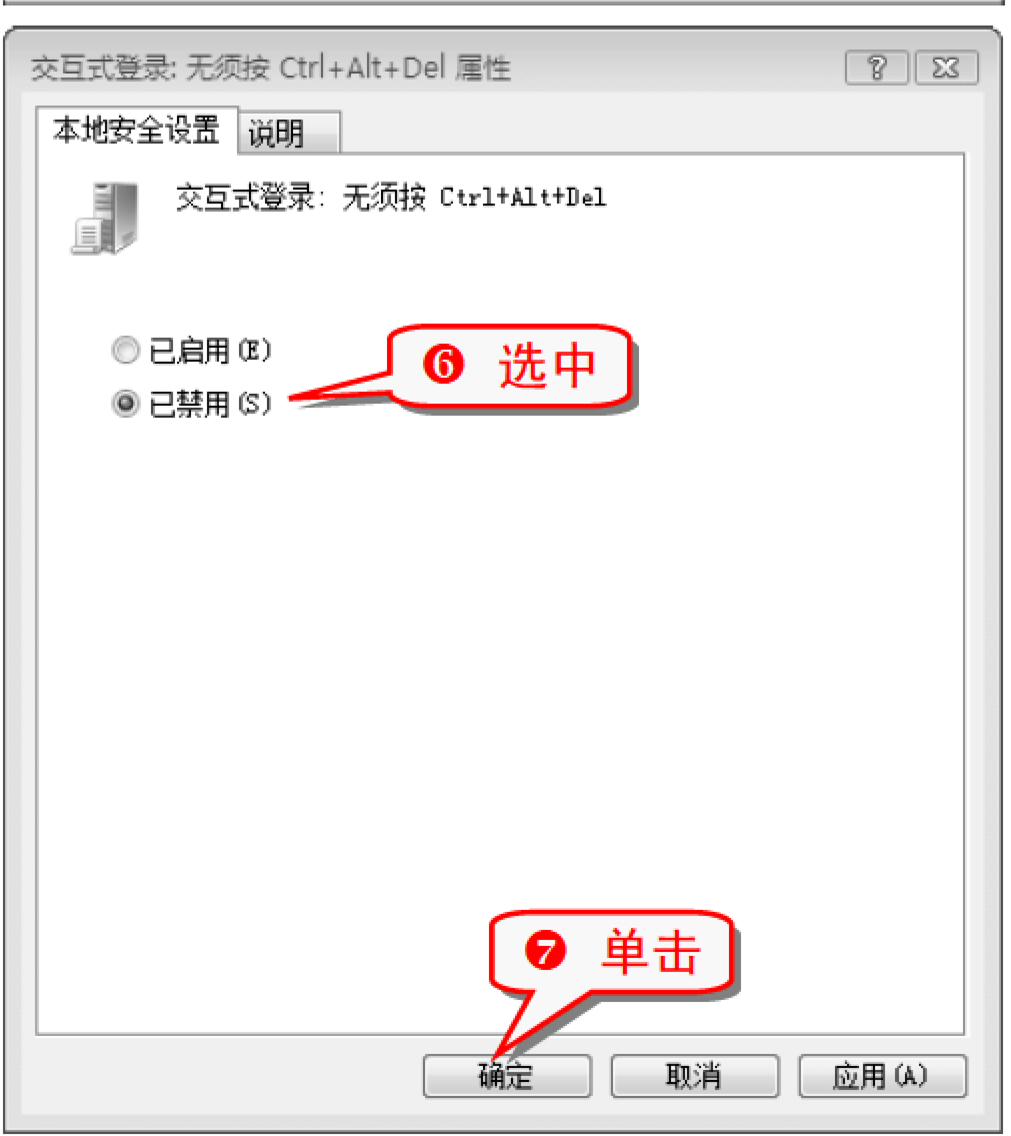
技巧107　启用 Ctrl＋Alt＋Delete 组合键交互式登录

登录之前按下 Ctrl＋Alt＋Delete 组合键可确保输入密码时安全进行通信。

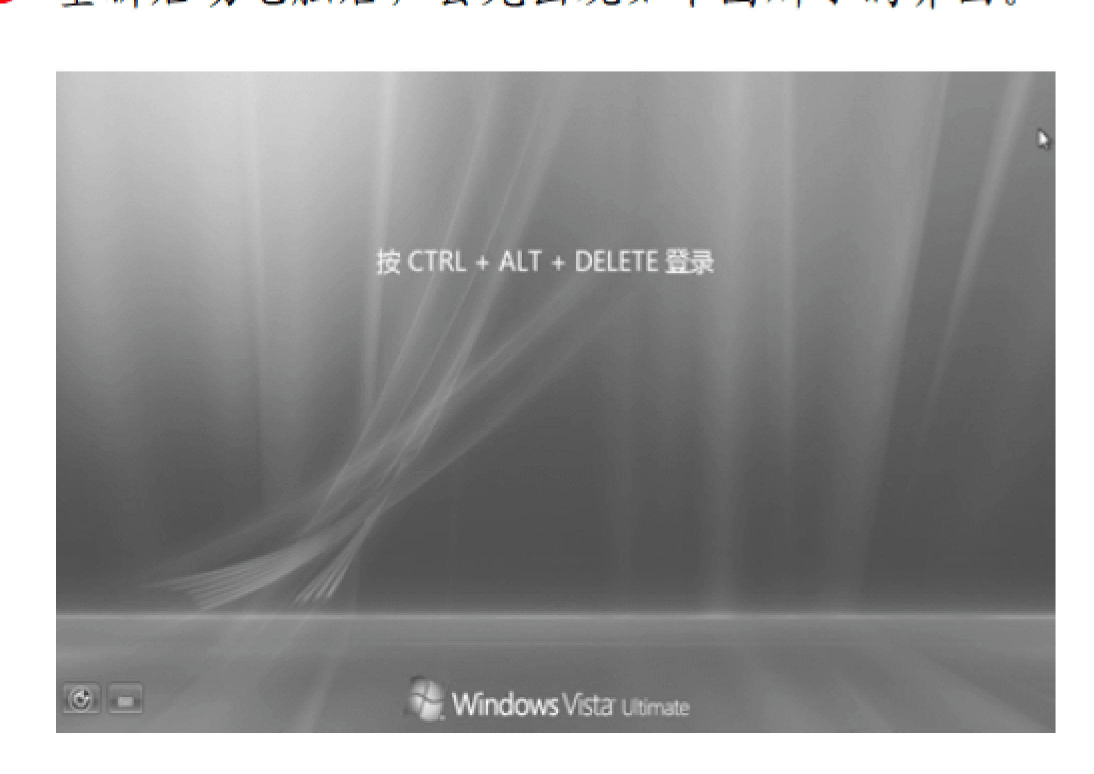
❶ 按下 ⊞ +R 组合键，弹出“运行”对话框。







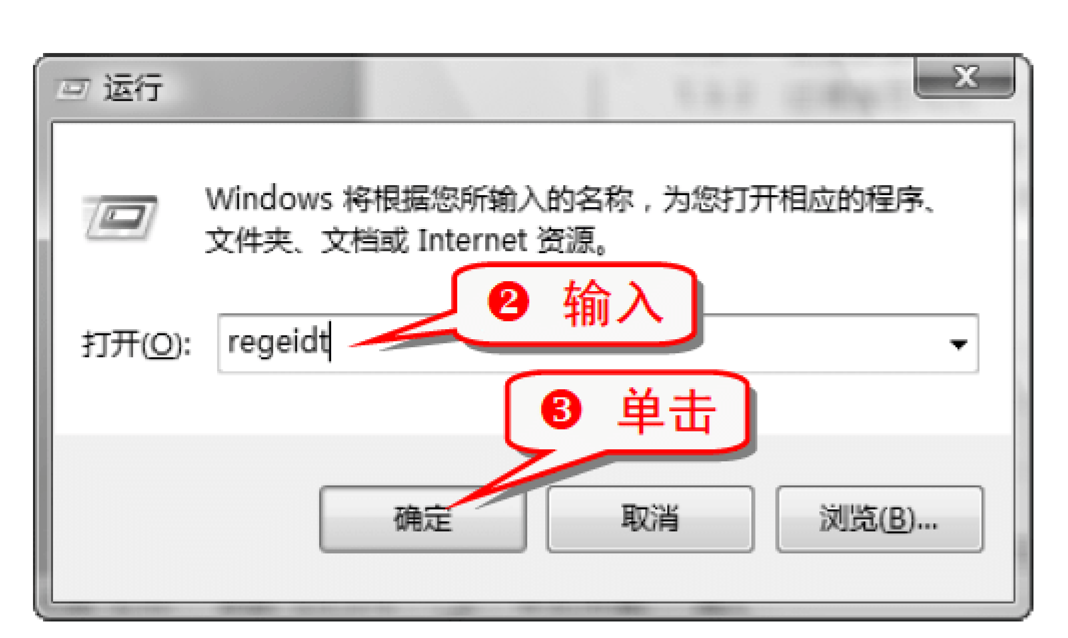
❽ 重新启动电脑后，会先出现如下图所示的界面。



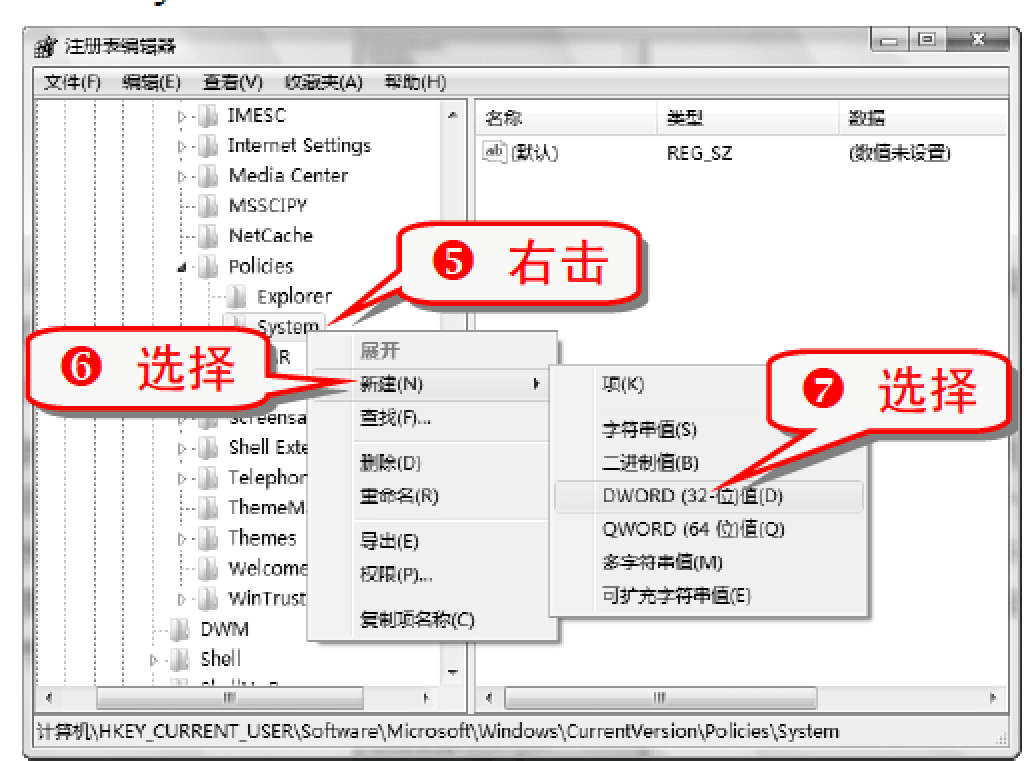
技巧108　禁用注册表编辑器

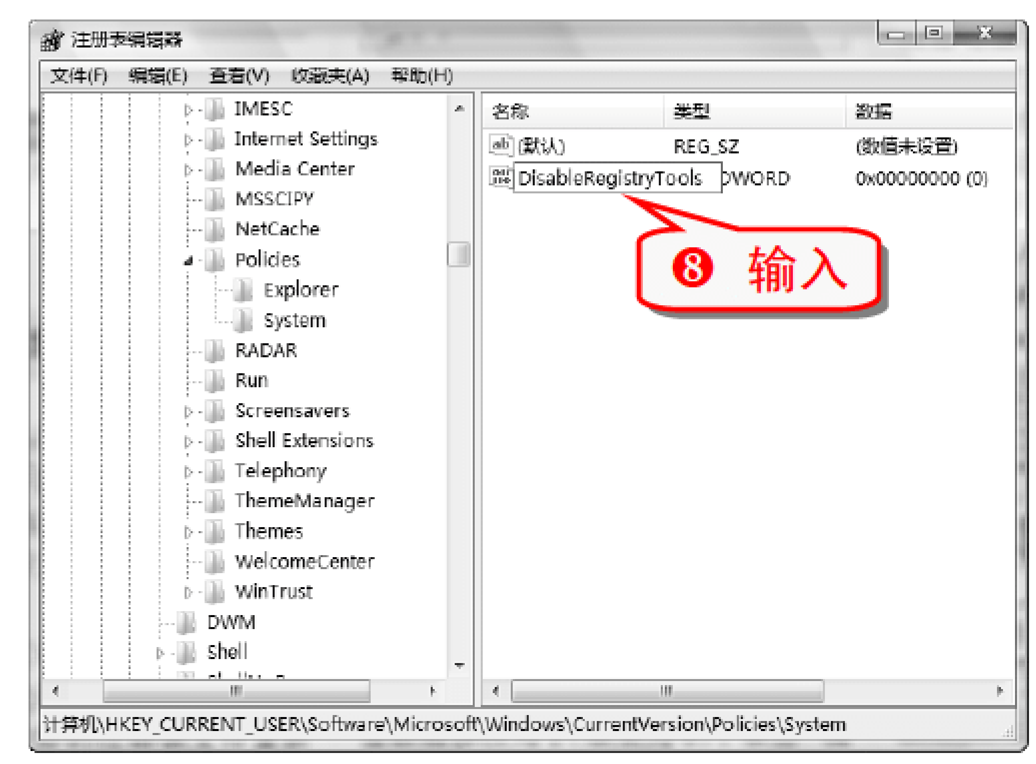
禁用注册表编辑器可以避免本地注册表被恶意修改，这样可以很好地维护系统的安全。

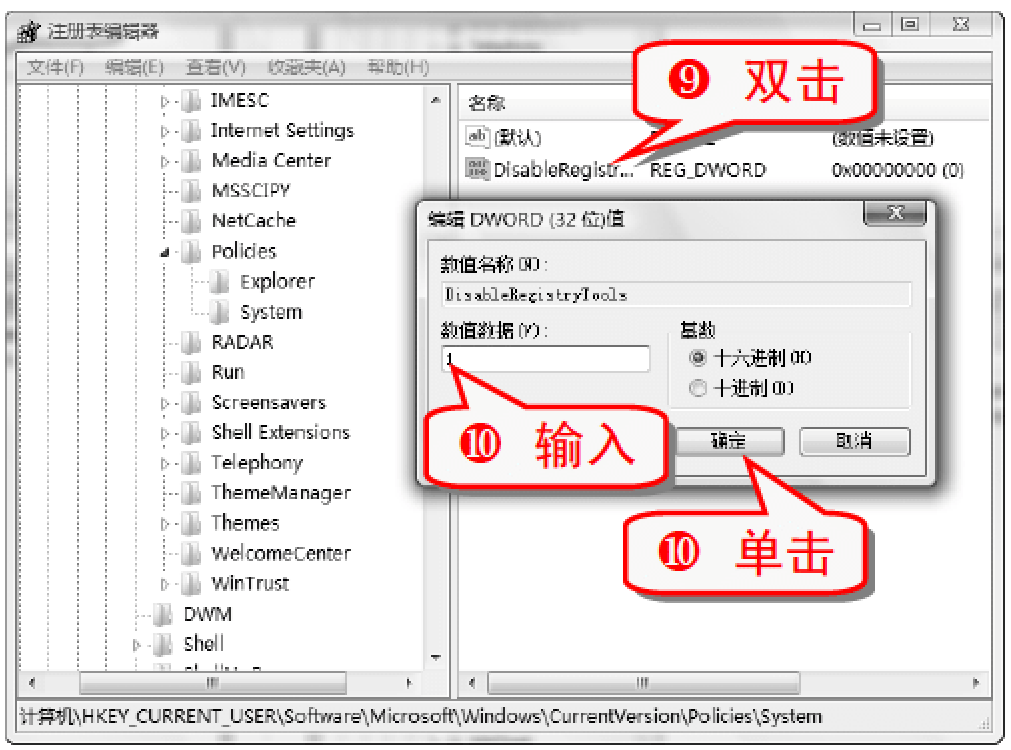
❶ 按下 ⊞ +R 组合键，弹出“运行”对话框。



❹ 展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System 分支，如果在 Policies 下面没有分支 System 项，新建一项，将其命名为 System。



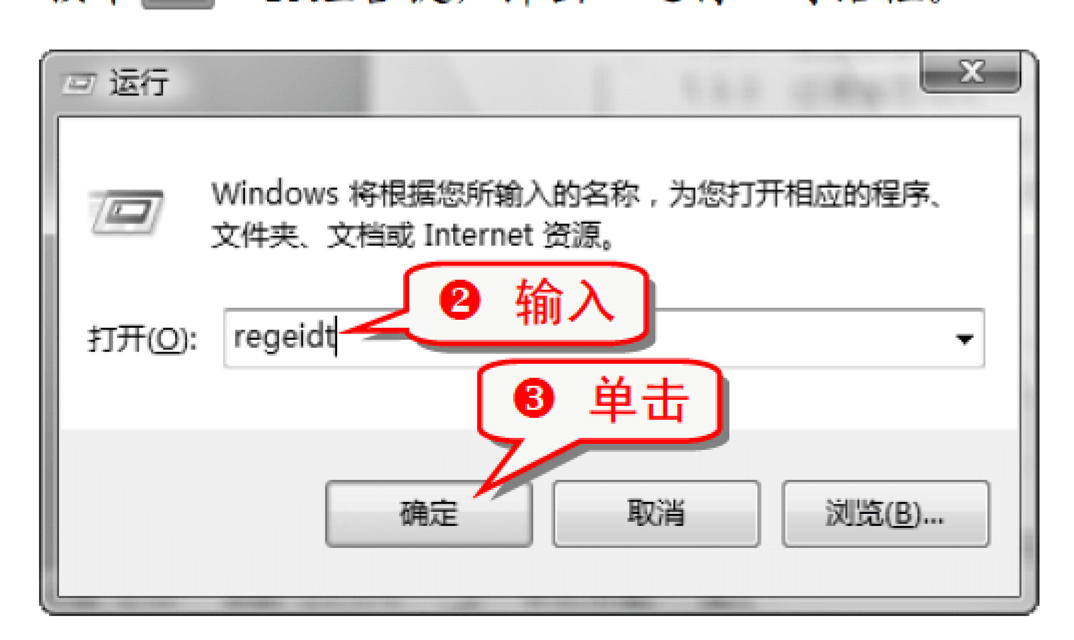




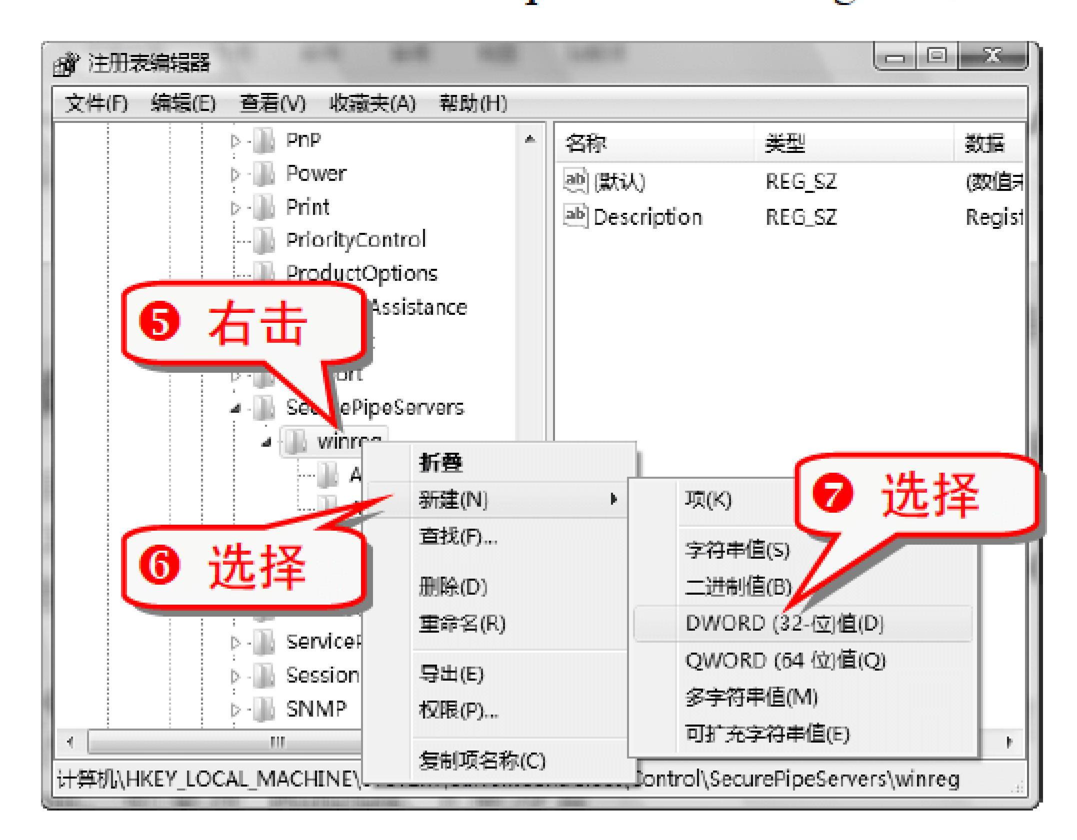
技巧109 禁止远程修改注册表

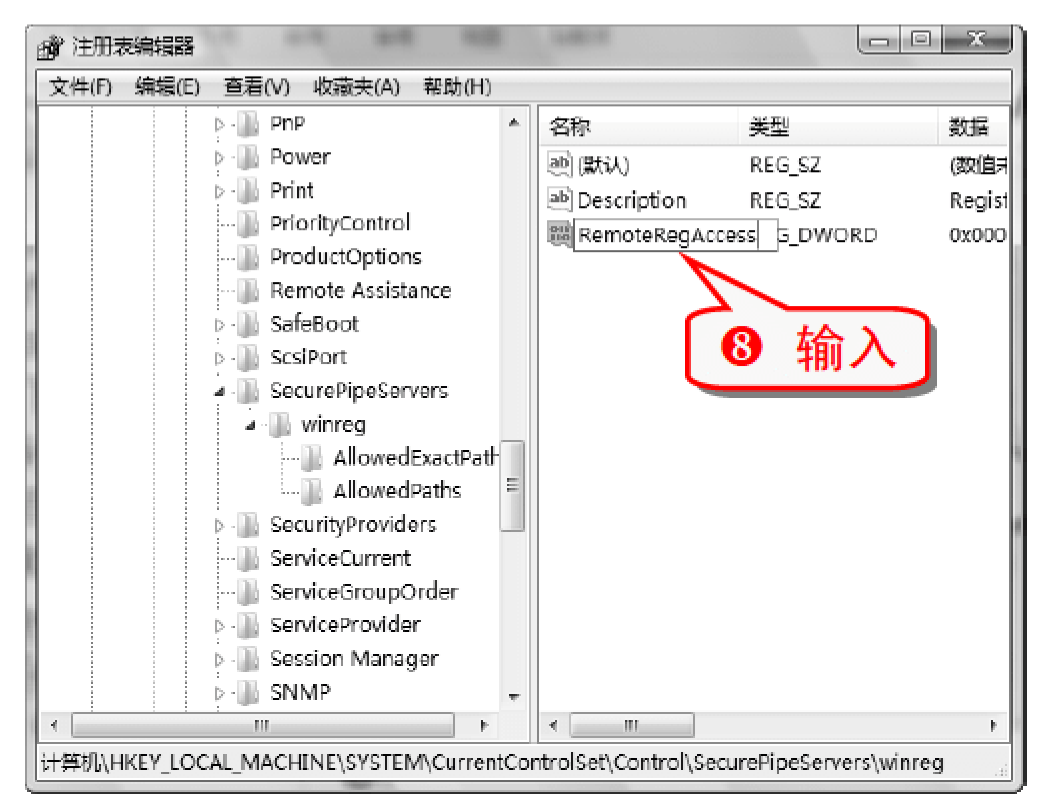
在这个黑客盛行的时代，很多不法之徒经常通过远程访问的方式对被攻击电脑的注册表进行修改，从而达到控制对方电脑的目的。为了增强电脑的安全性，可以将注册表类型设置为禁止远程修改。

❶ 按下 ⊞ + R 组合键，弹出“运行”对话框。



❹ 展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg 分支。





❾ 双击 RemoteRegAccess 选项，在“编辑 DWORD(32 位)值”窗口的文本框中输入 1，单击“确定”按钮。

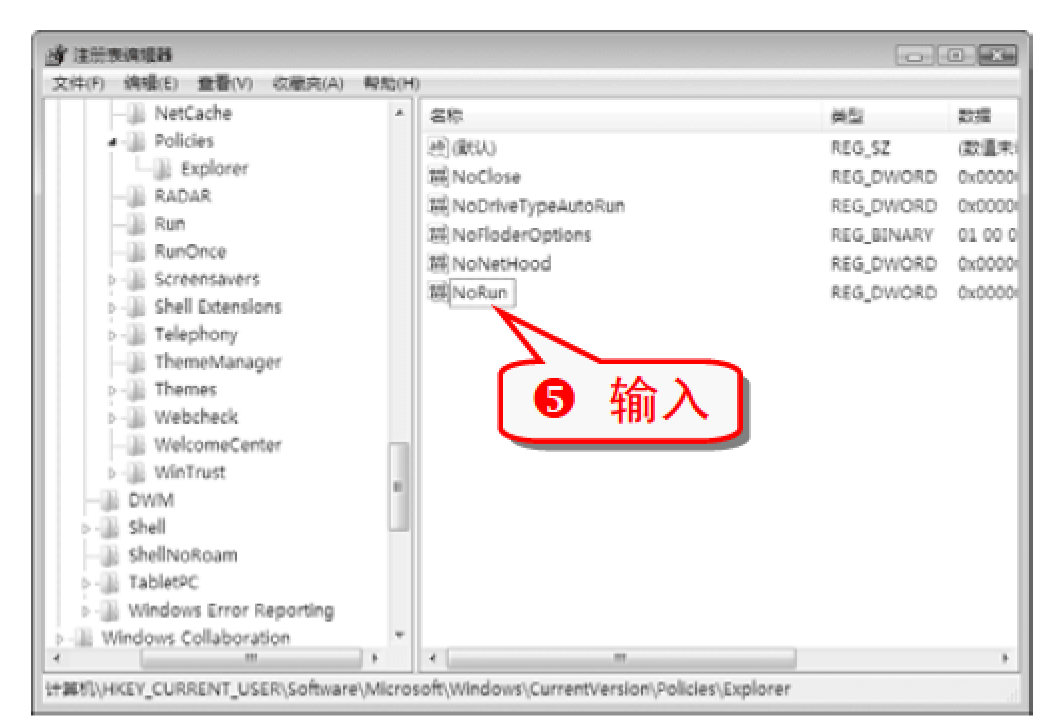


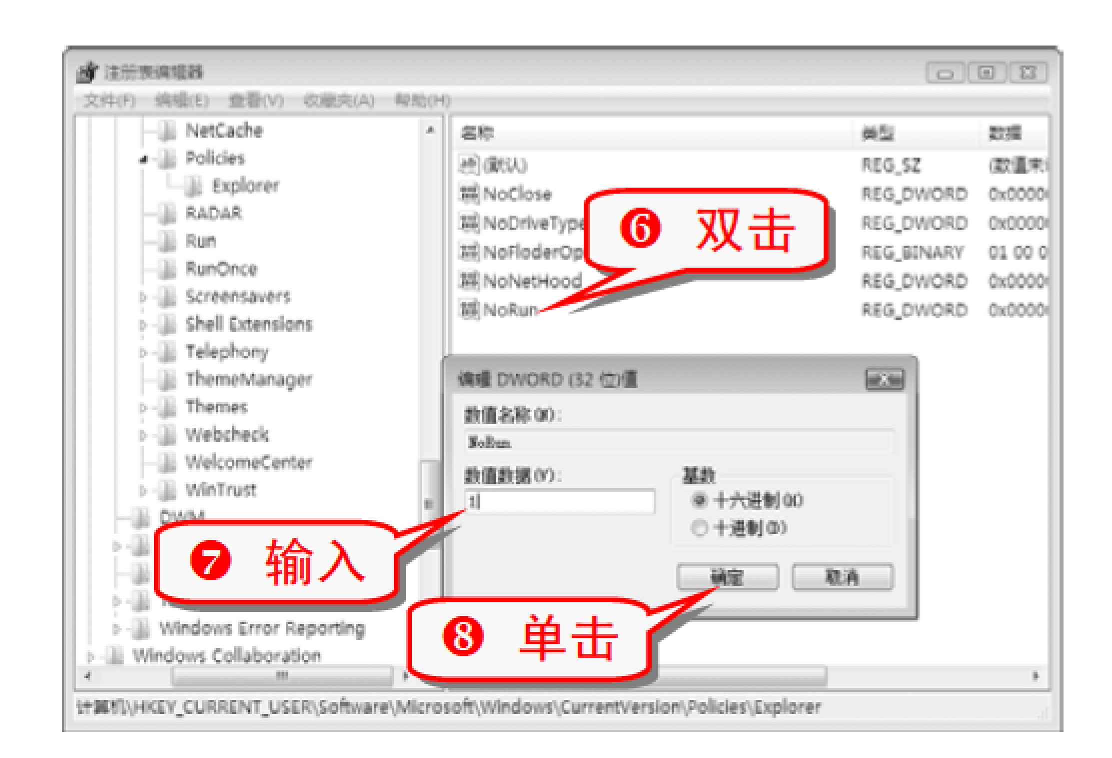
技巧110　禁用“运行”对话框

通过“运行”对话框可以访问任何程序和文件夹，导致系统的安全性大大降低，低安全等级用户可以考虑禁用“运行”功能。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支。







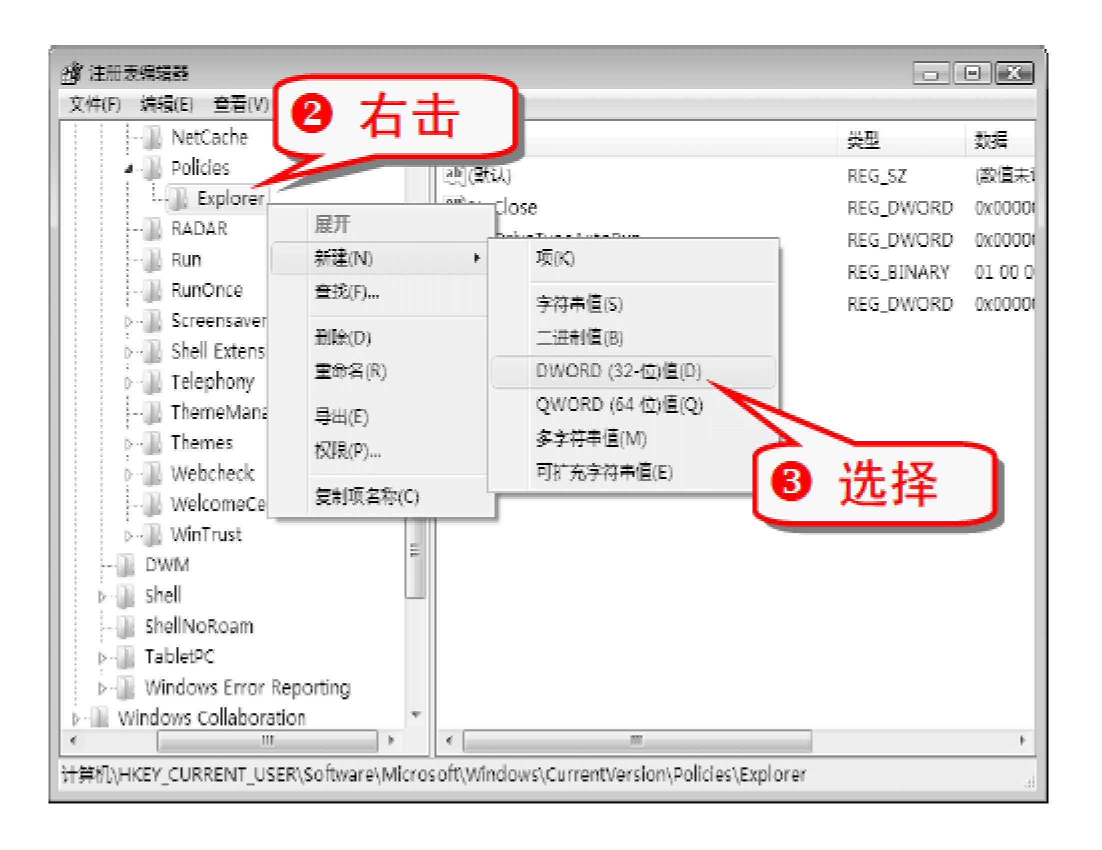


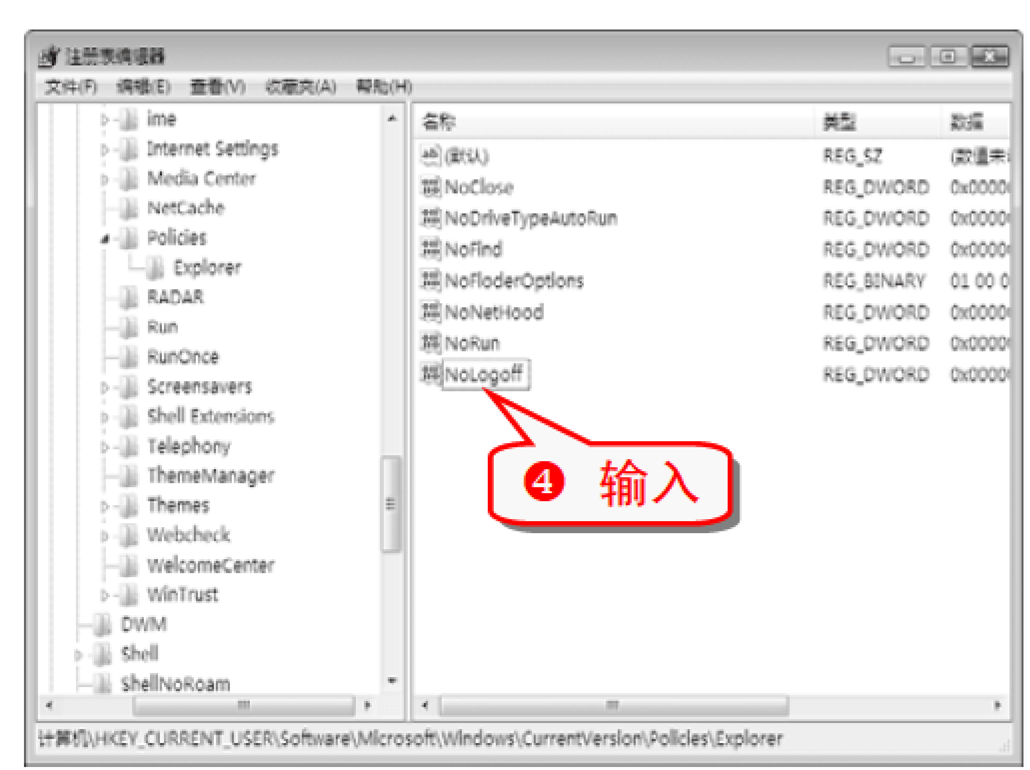
要重新启动或注销系统，设置才会生效。

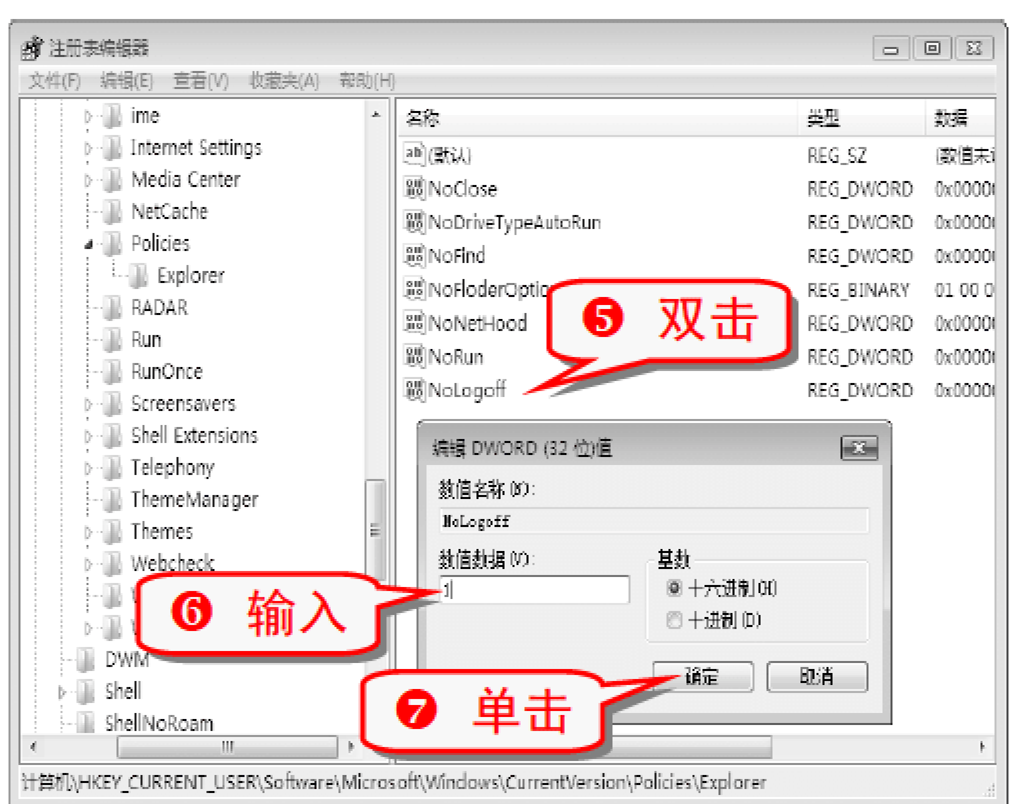
技巧111　屏蔽按下Ctrl+Alt+Delete组合键弹出的对话框中的注销功能

通过修改注册表可以屏蔽按下 Ctrl+Alt+Delete 组合键后弹出的对话框中的注销功能。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支。









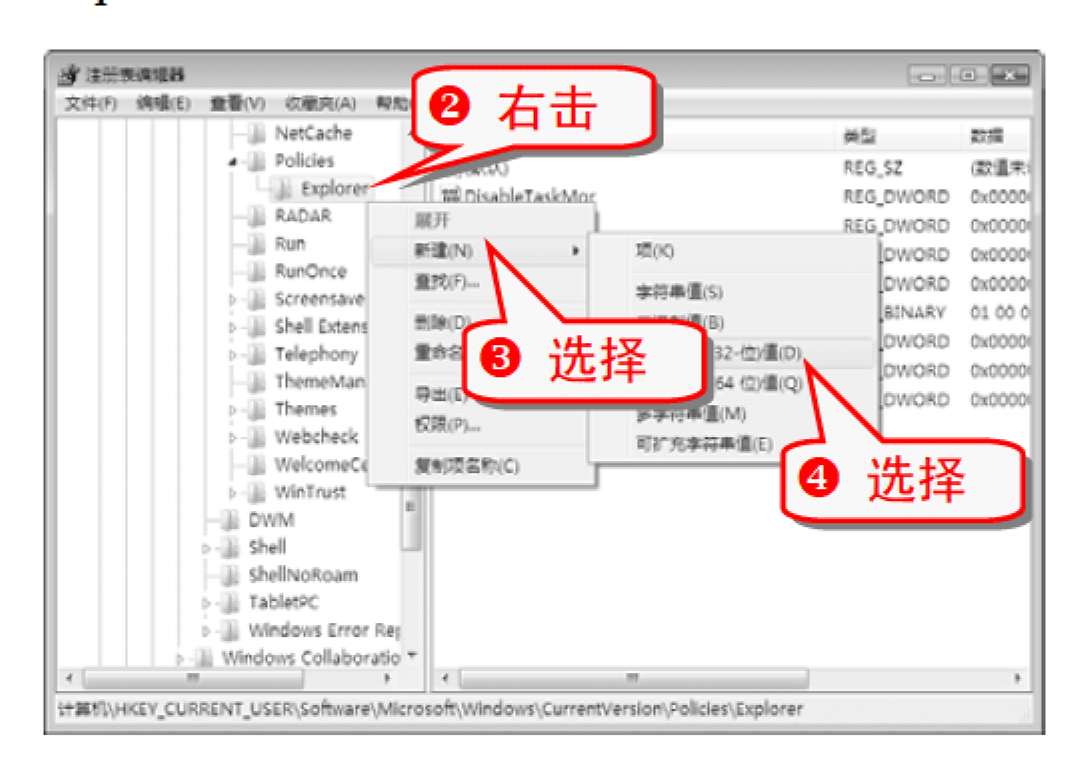
注 意 事 项

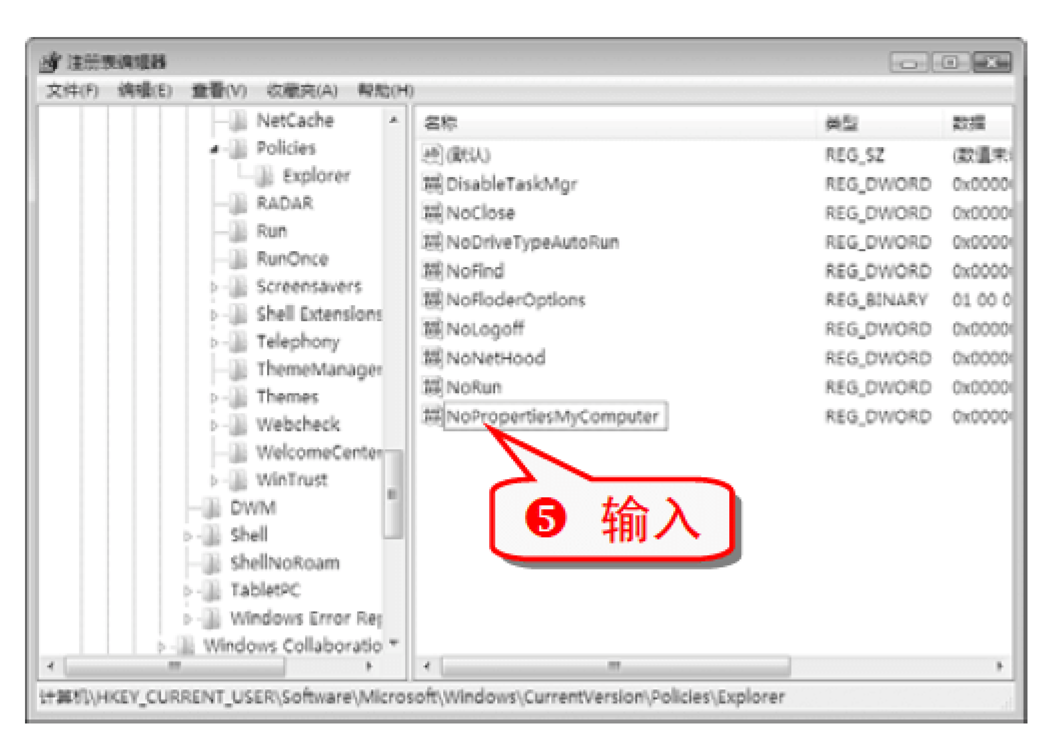
要重新启动或注销系统，设置才会生效。

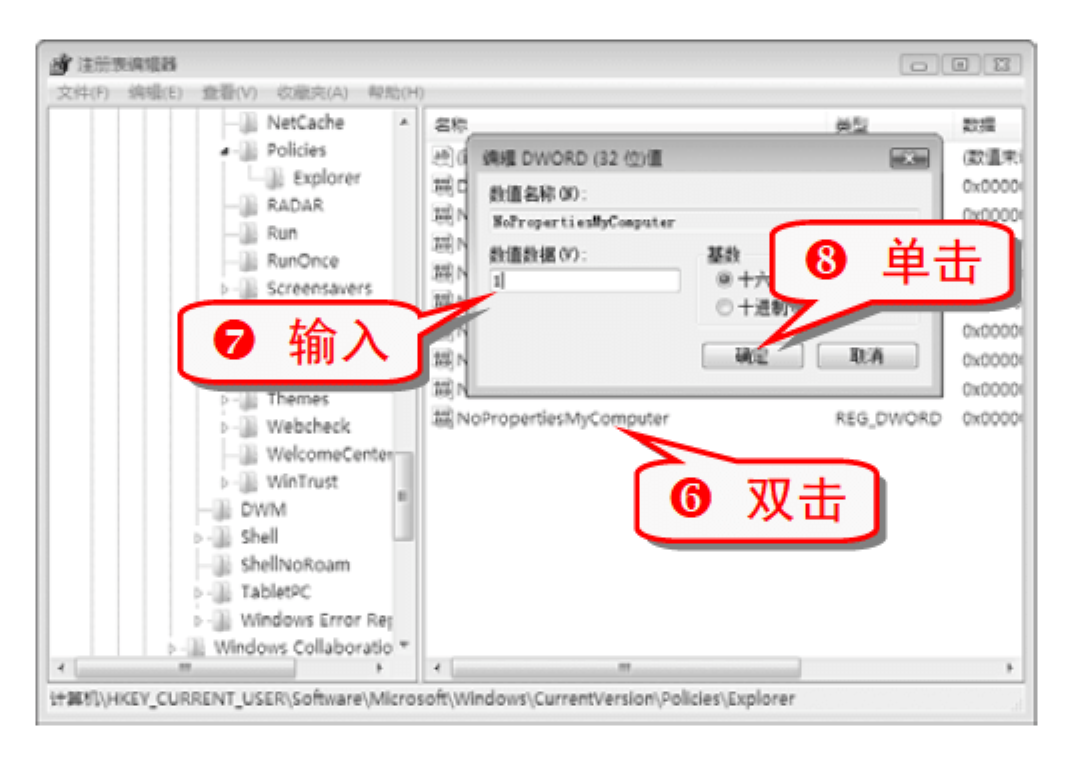
技巧112 从“计算机”快捷菜单中删除“属性”选项

通过修改注册表可以删除右击“计算机”图标后弹出的快捷菜单中的“属性”选项。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支。











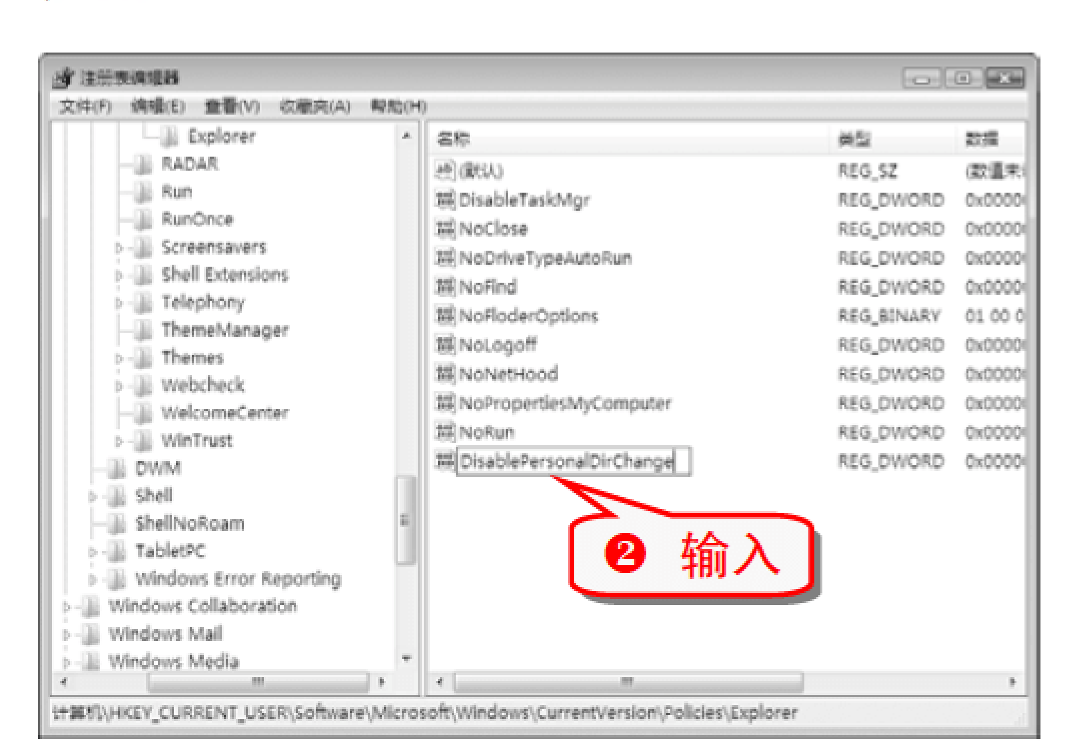
注 意 事 项

将 NoPropertiesMyComputer 的键值设置为 0 可以显示“属性”。设置在注销或重新启动后生效。

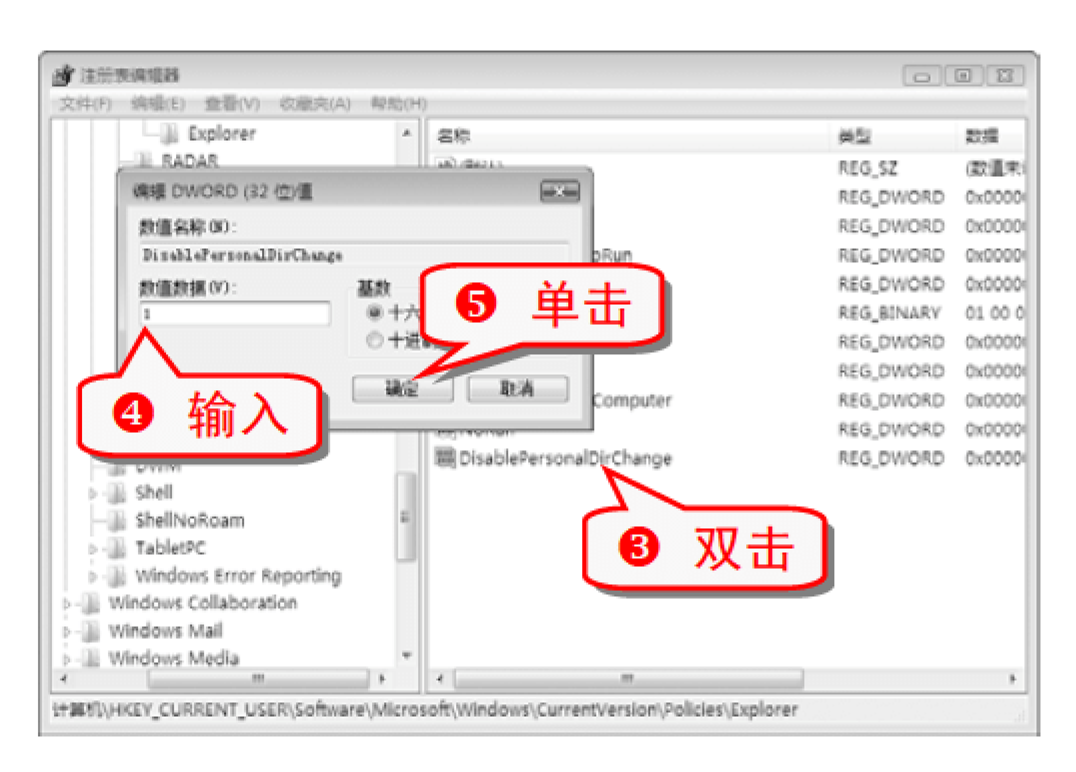
技巧113 禁止更改“文档”文件夹位置

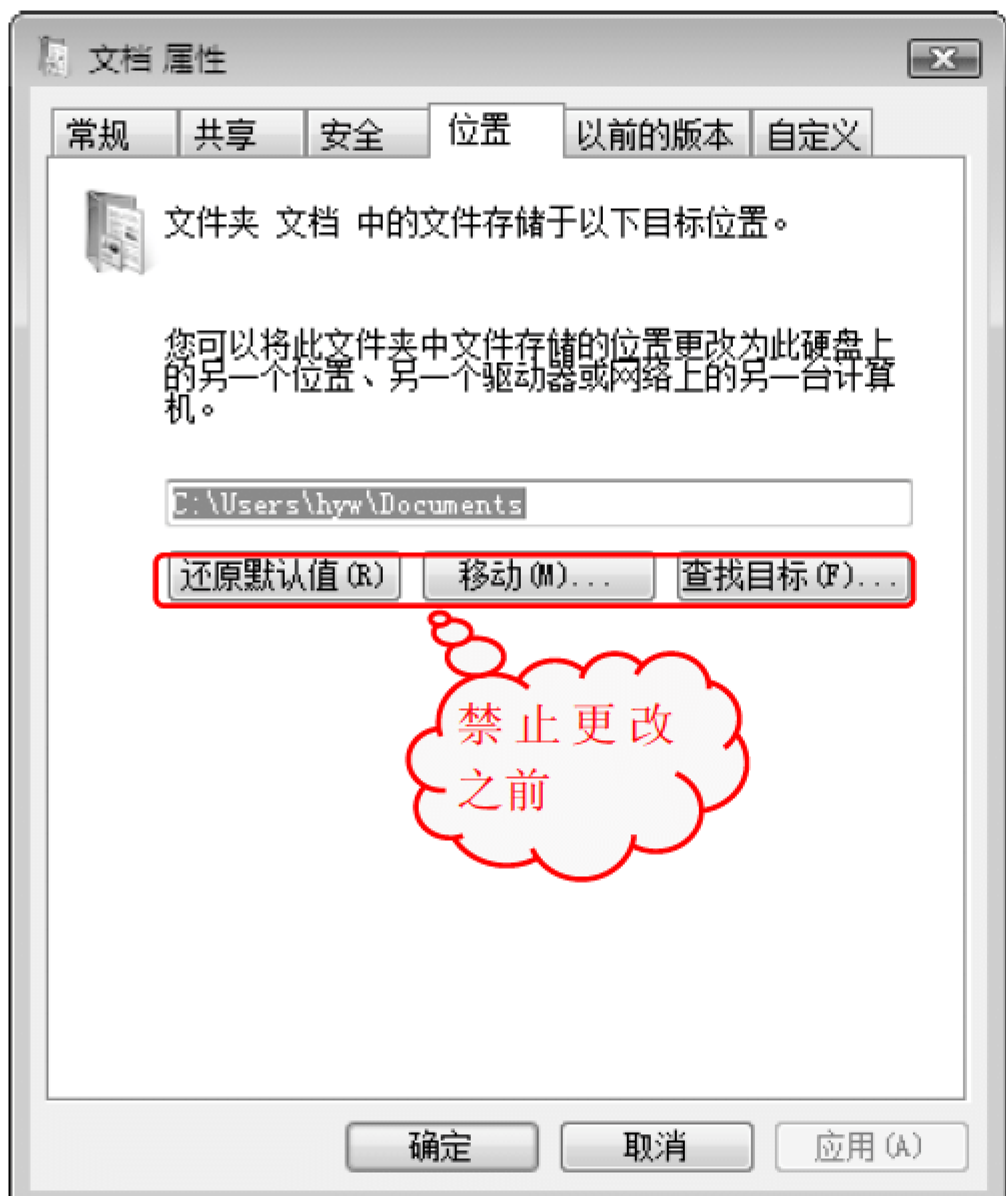
通过修改注册表可以禁止更改“文档”文件夹位置。

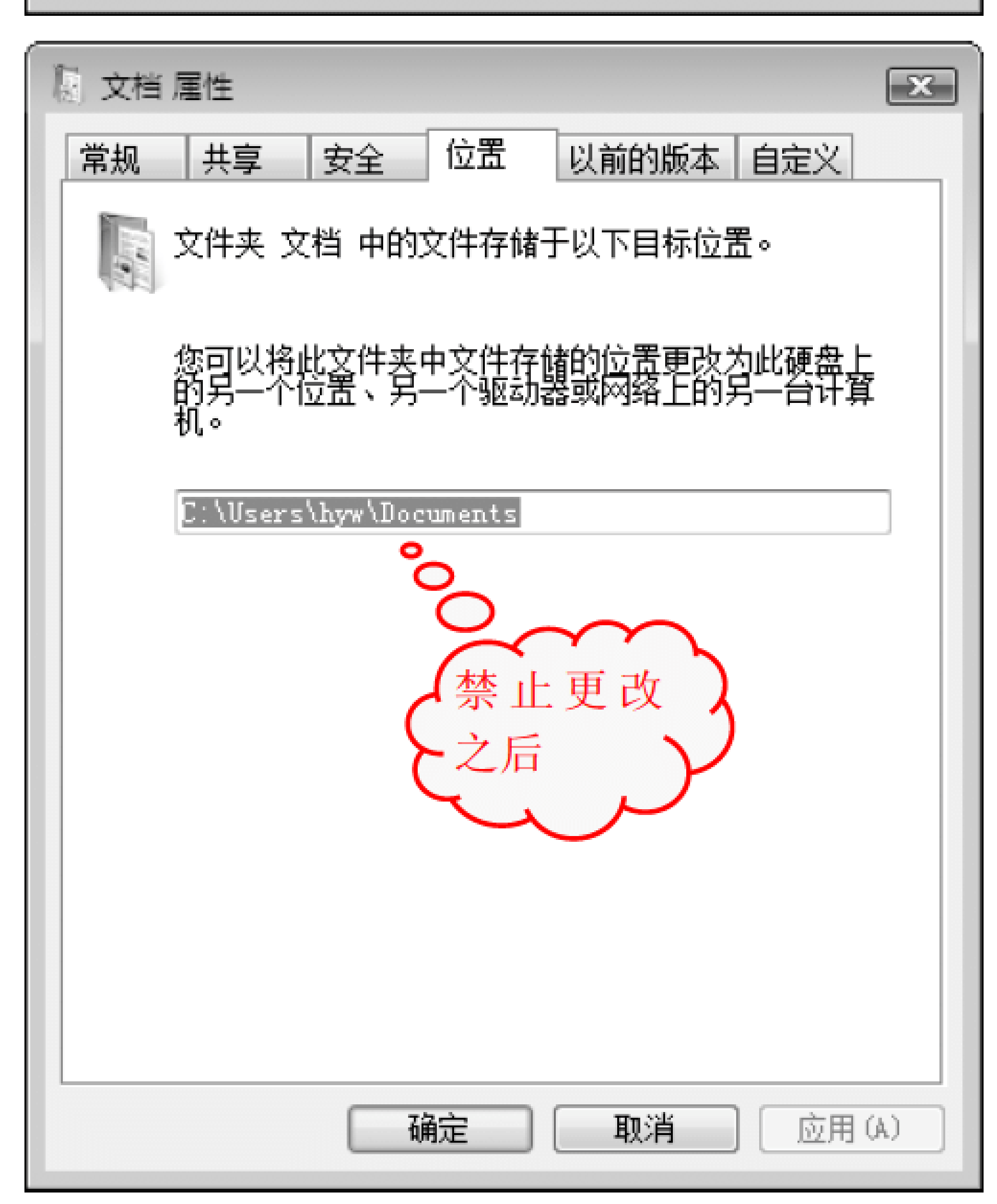
❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支，新建一个类型为 DWORD(32 位)的键值项。











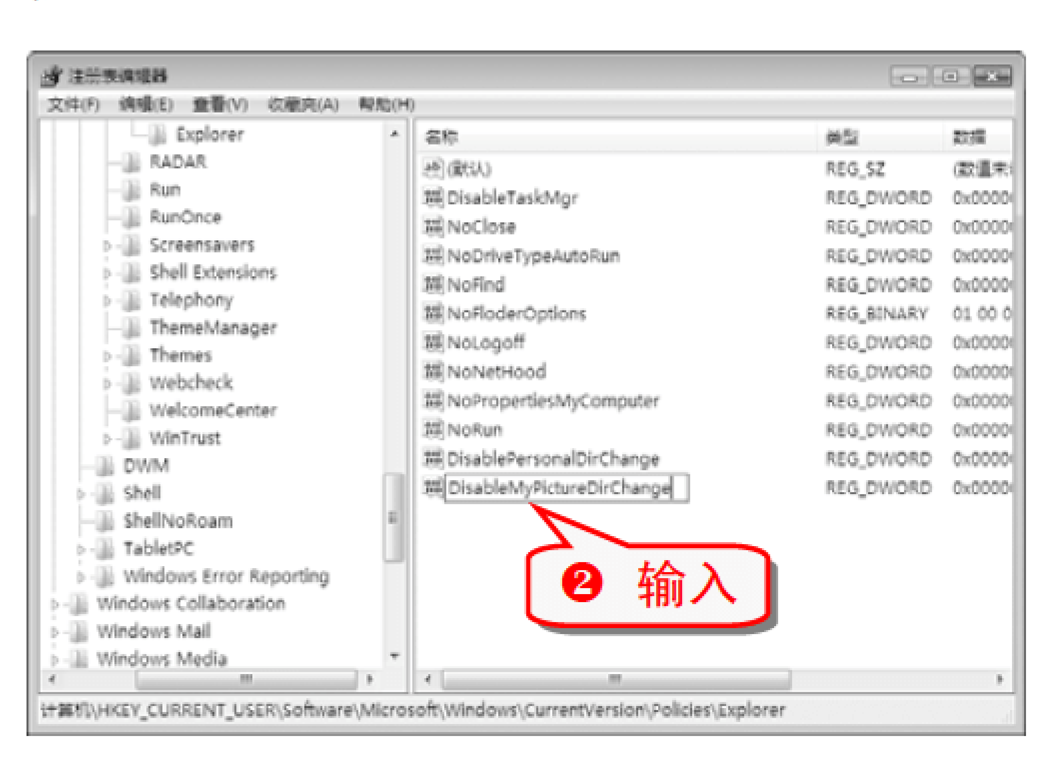
注　意　事　项

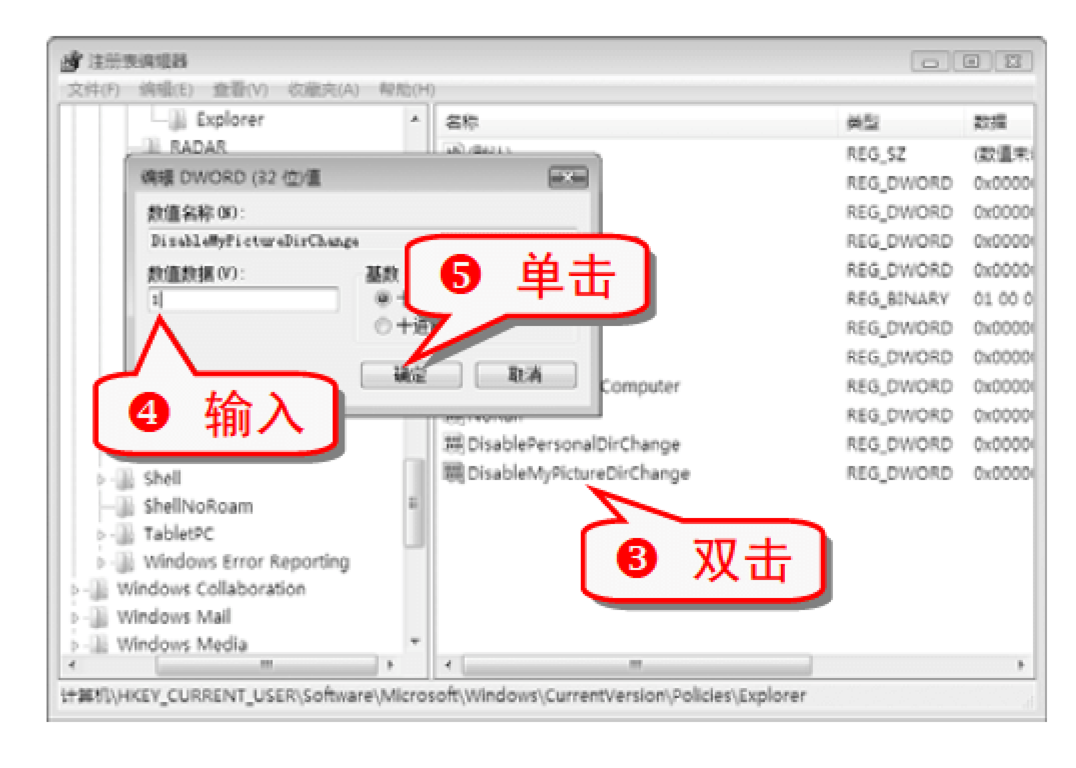
将 DisablePersonalDirChange 的键值设置为 0，则允许更改“文档”文件夹的位置。设置在注销或重新启动后生效。

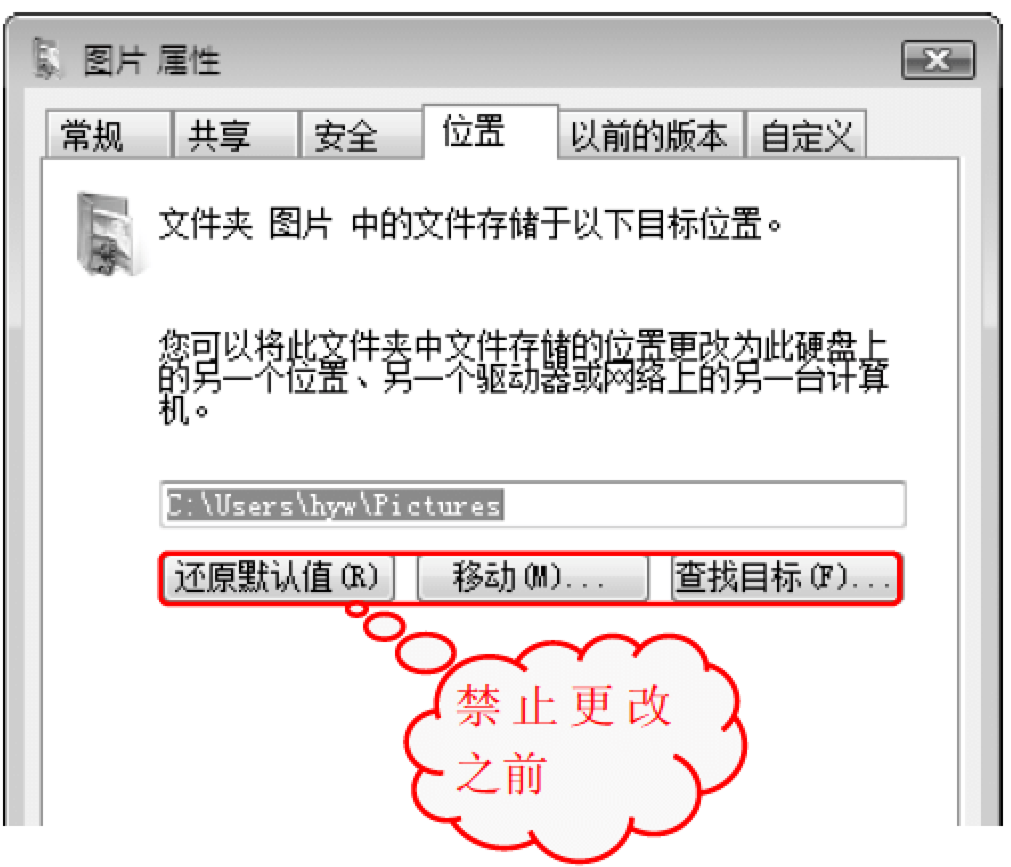
技巧114　禁止更改“图片”文件夹位置

通过修改注册表可以禁止更改“图片”文件夹位置。

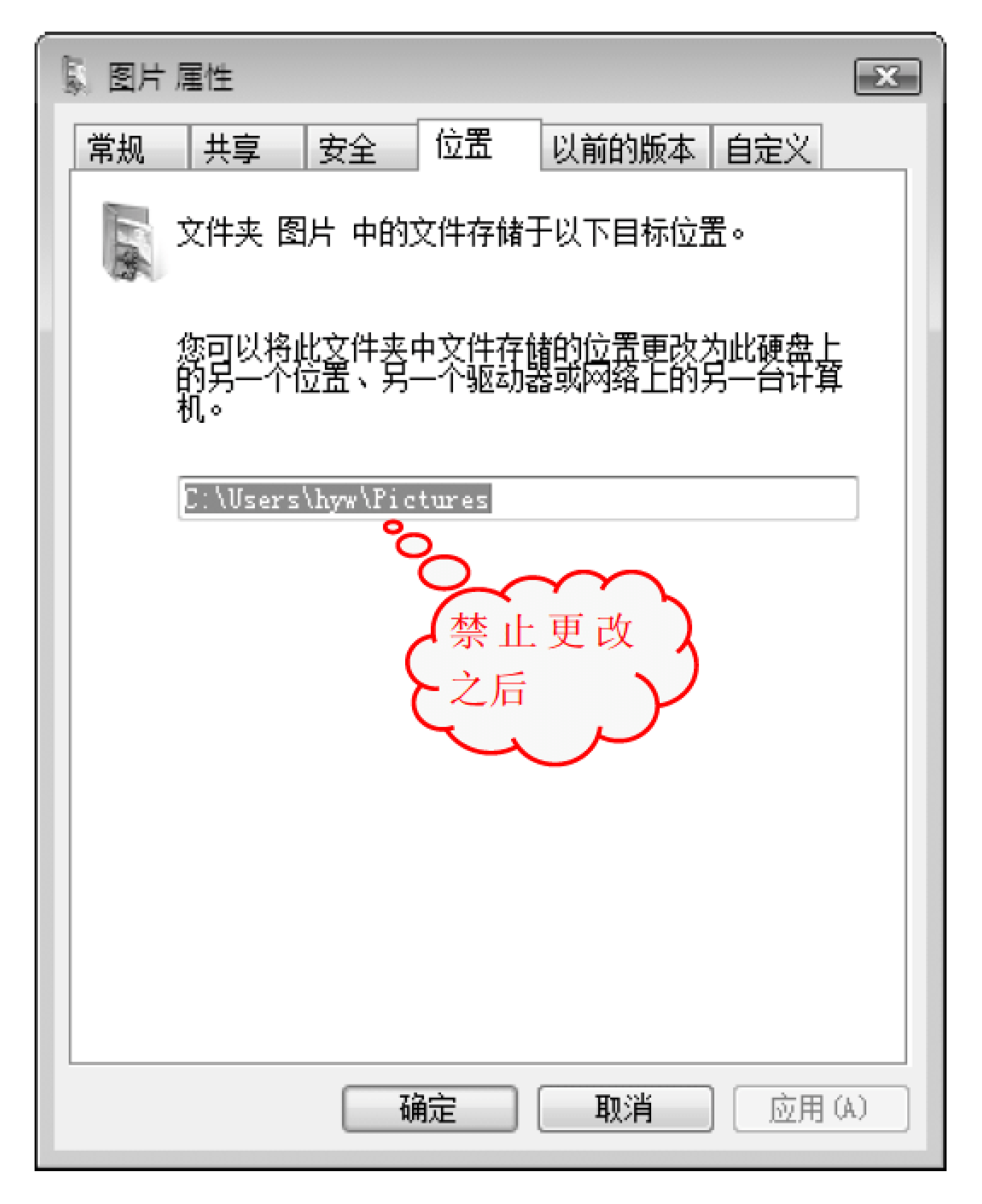
❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支，新建一个类型为 DWORD(32 位)的键值项。











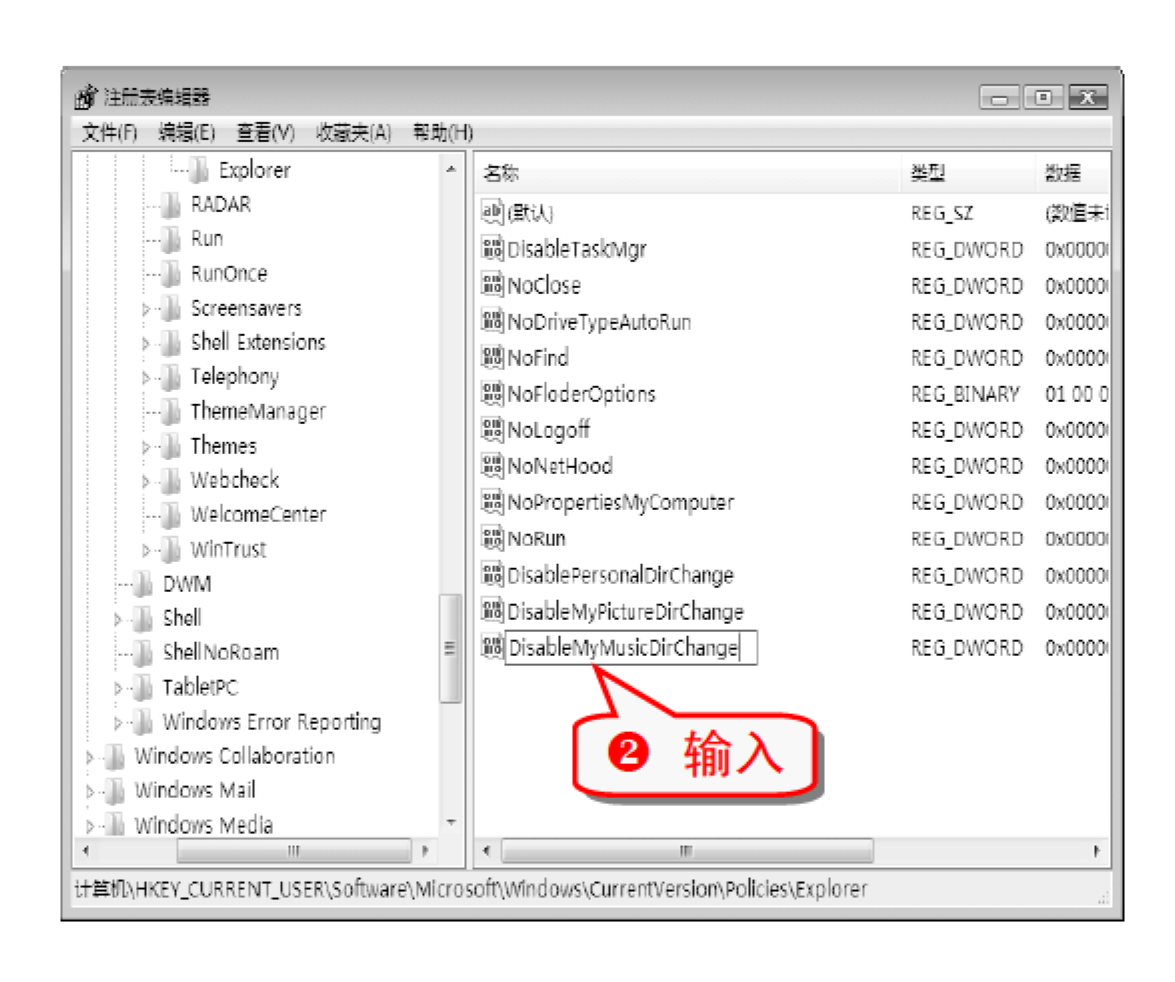


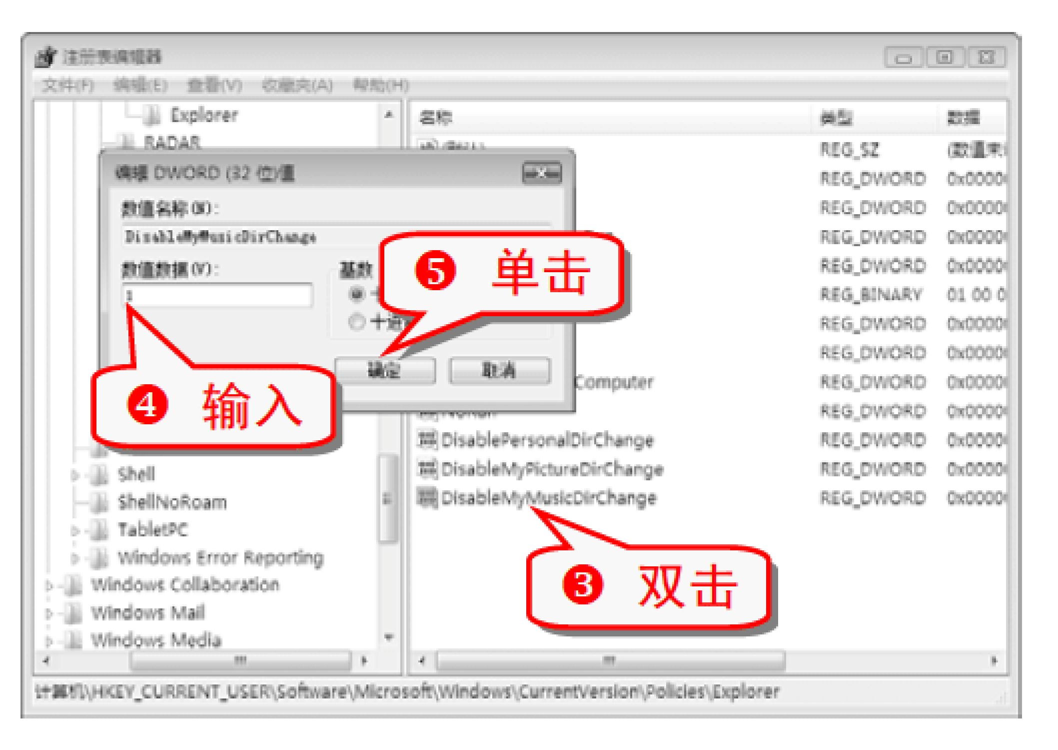
将 DisableMyPicturesDirChange 的键值设置为 0，则允许更改“图片”文件夹的位置。设置在注销或重新启动后生效。

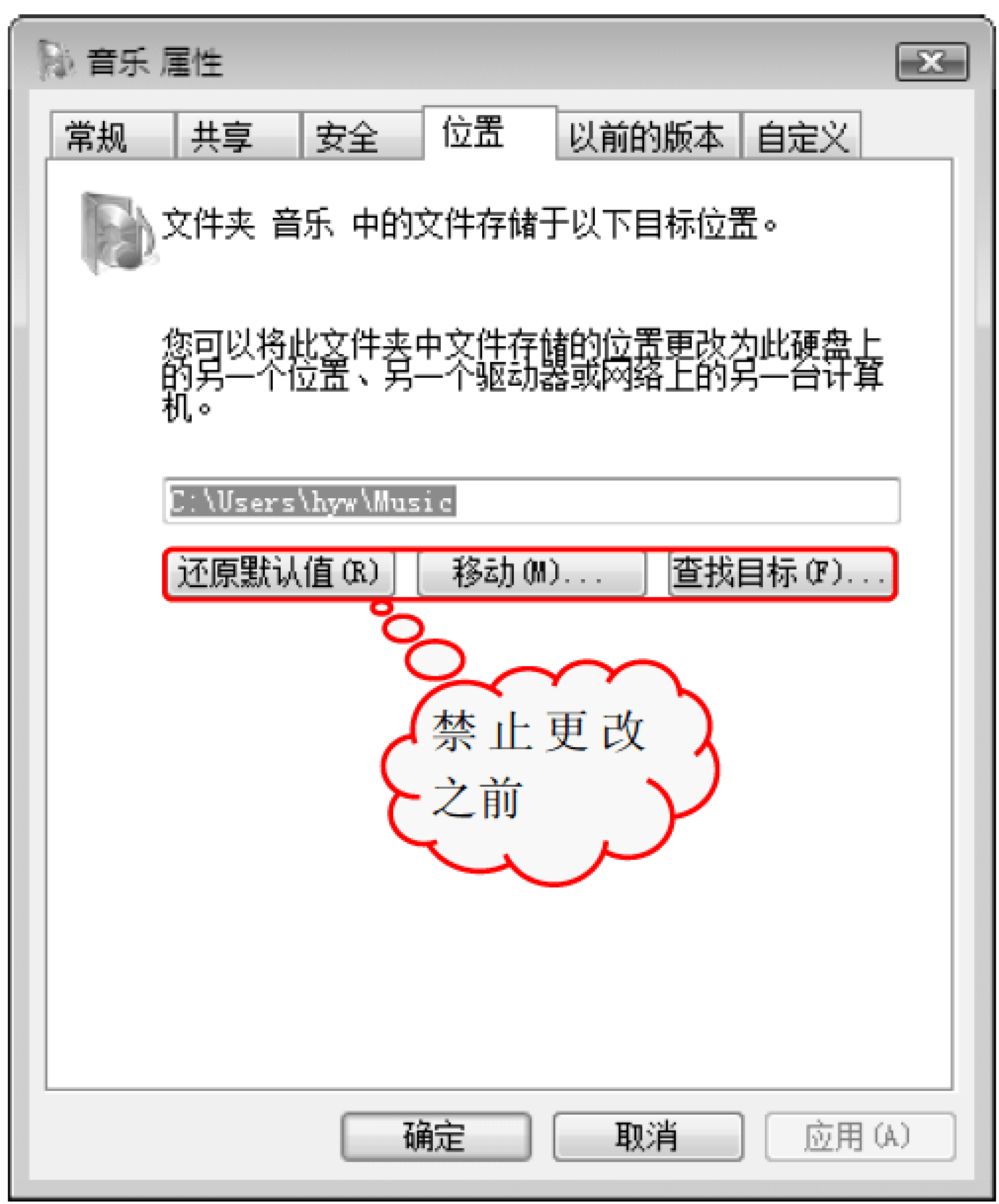
技巧115 禁止更改“音乐”文件夹位置

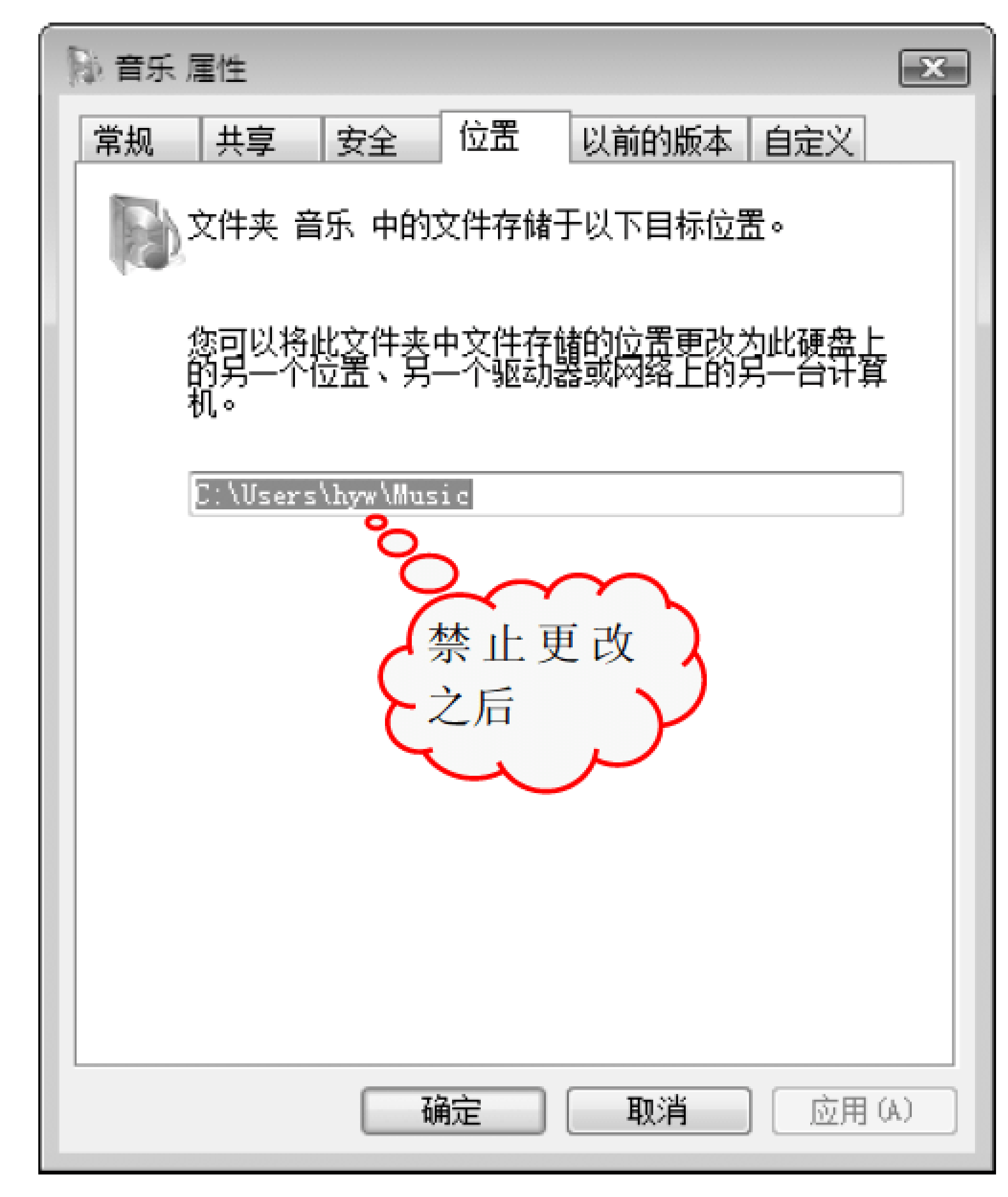
通过修改注册表可以禁止更改“音乐”文件夹位置。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支，新建一个类型为 DWORD(32 位)的键值项。













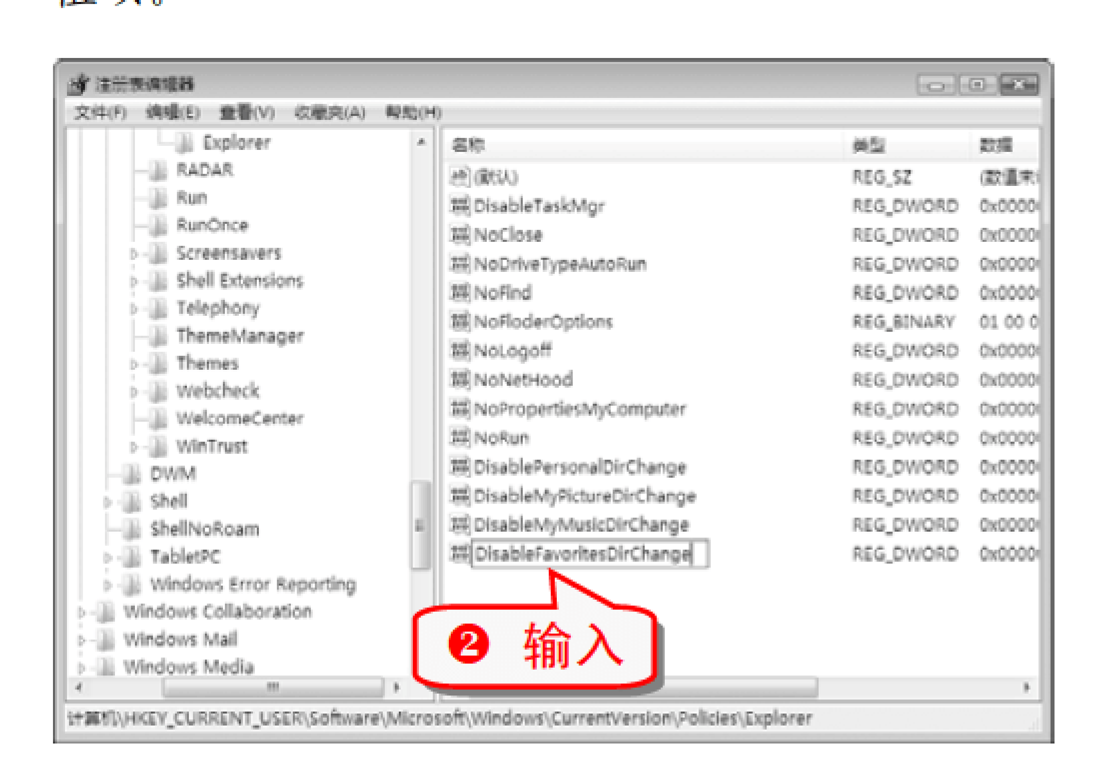

注　意　事　项

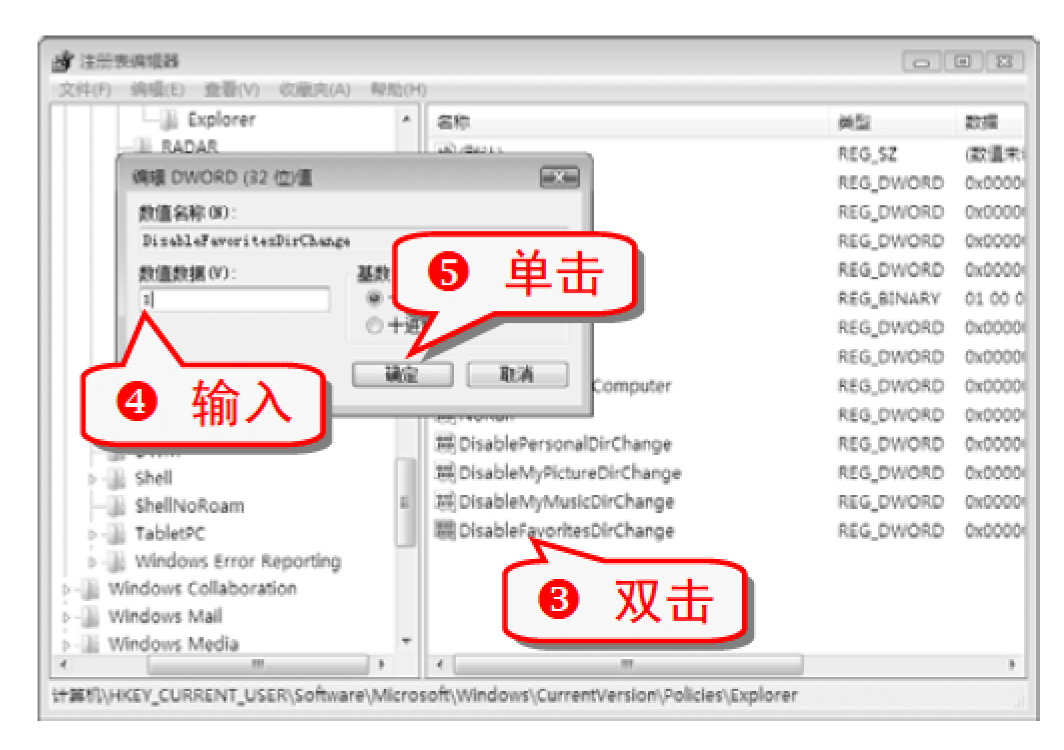
将 DisableMyMusicDirChange 的键值设置为 0，则允许更改“音乐”文件夹的位置。设置在注销或重新启动后生效。

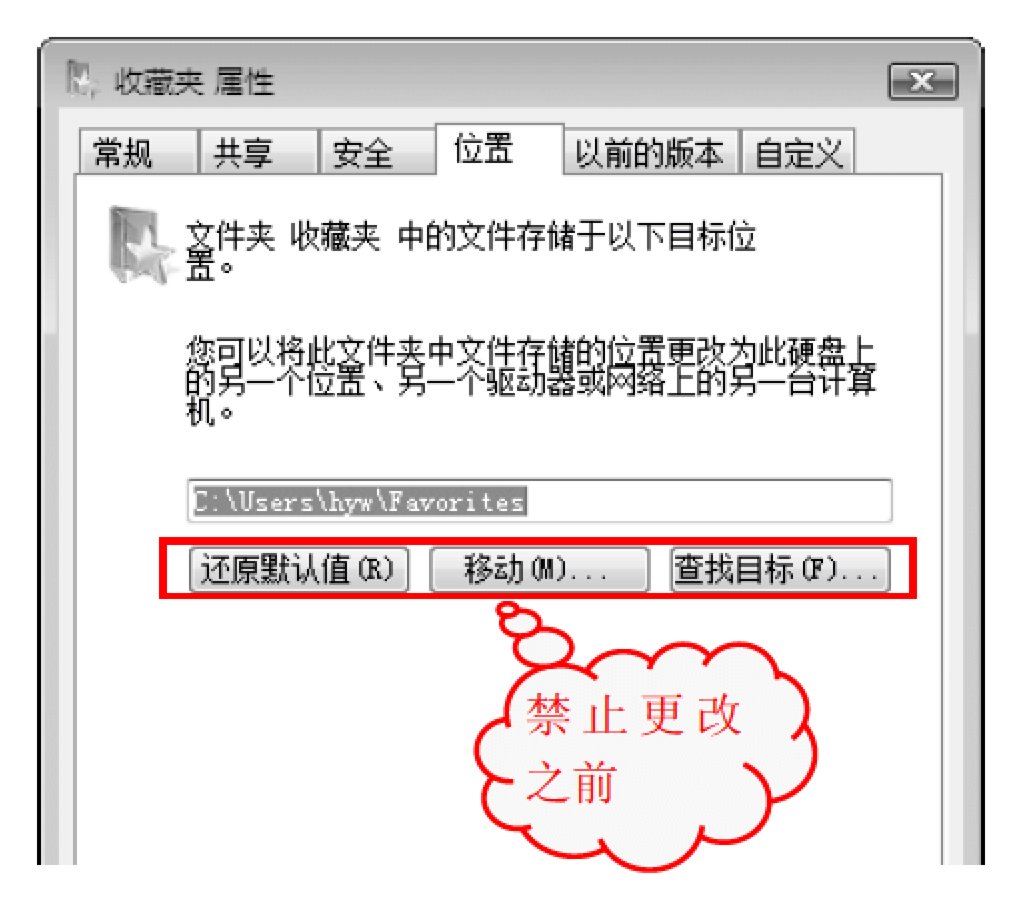
技巧116　禁止更改“收藏夹”文件夹位置

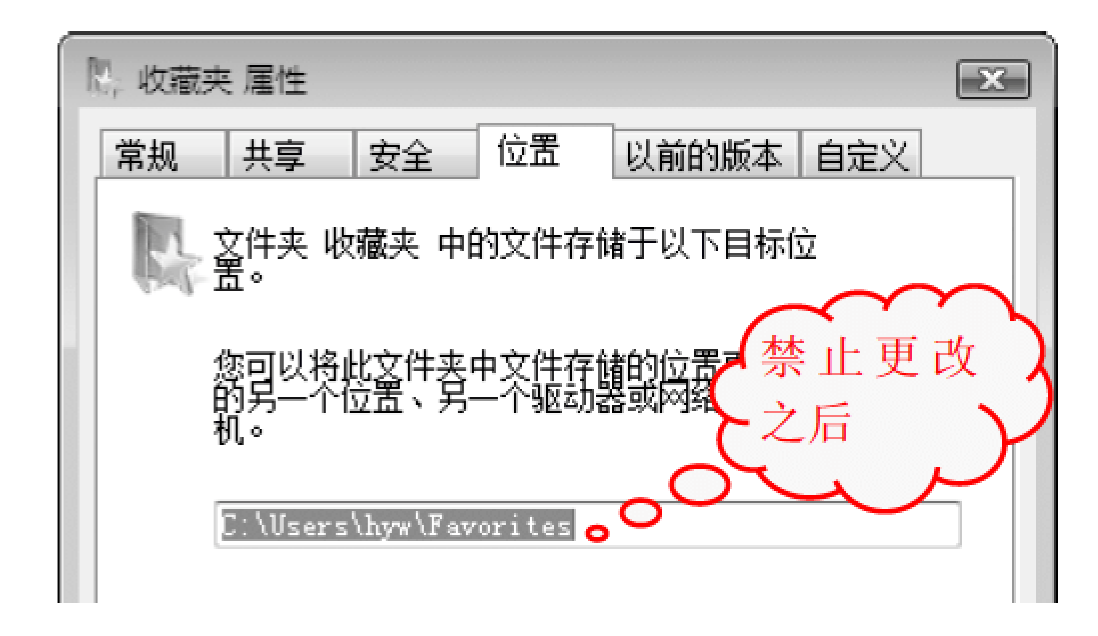
通过修改注册表可以禁止更改“收藏夹”文件夹位置。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支，新建一个类型为 DWORD(32 位)的键值项。











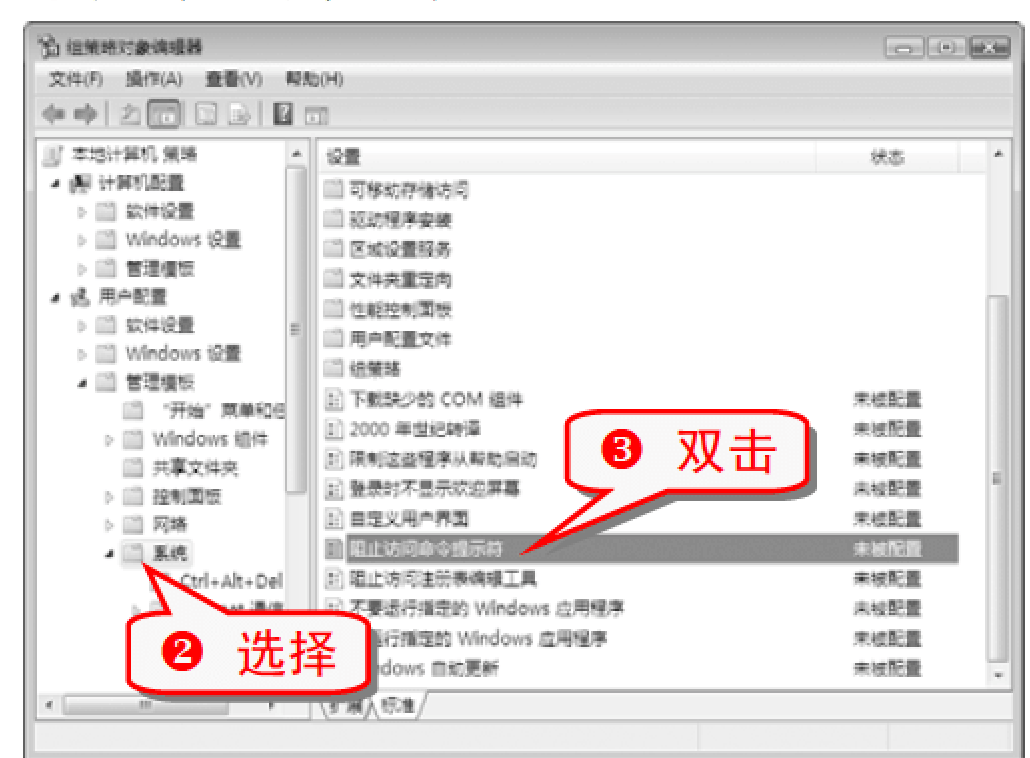
注　意　事　项

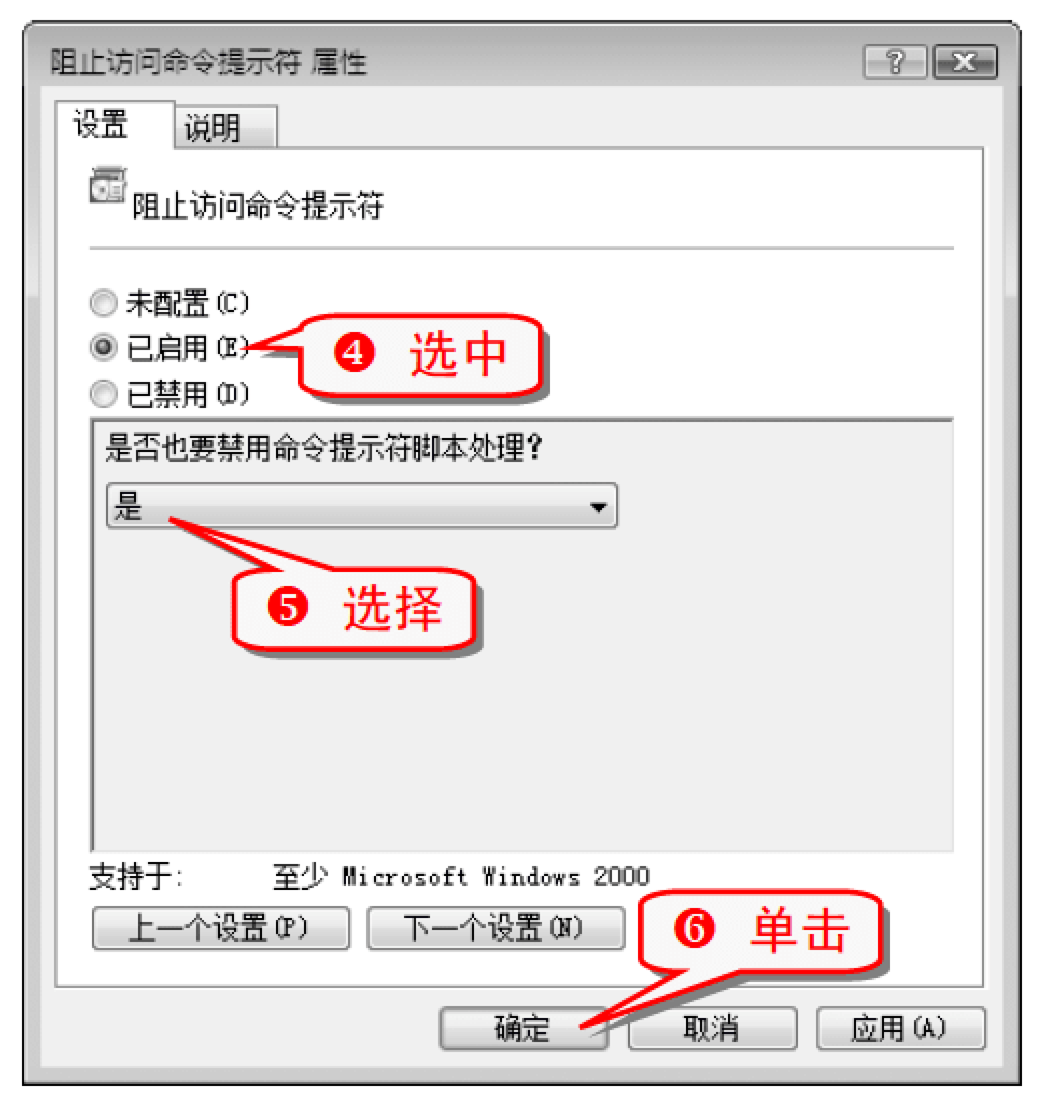
将 DisableFavoritesDirChange 的键值设置为 0，则允许更改“收藏夹”文件夹的位置。设置在注销或重新启动后生效。

技巧117　禁止使用命令提示符

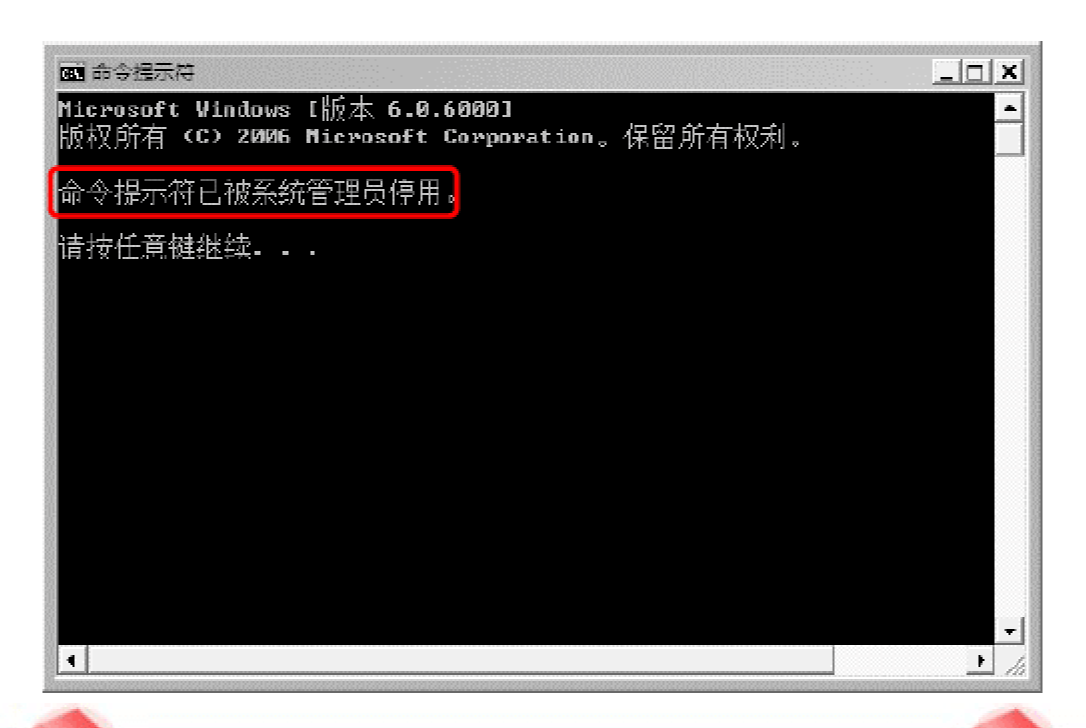
在命令提示符中使用一些命令会造成安全隐患，为了保证系统安全可以禁用此功能。

❶ 打开组策略对象编辑器。





❼ 打开“命令提示符”窗口。



知 识 补 充

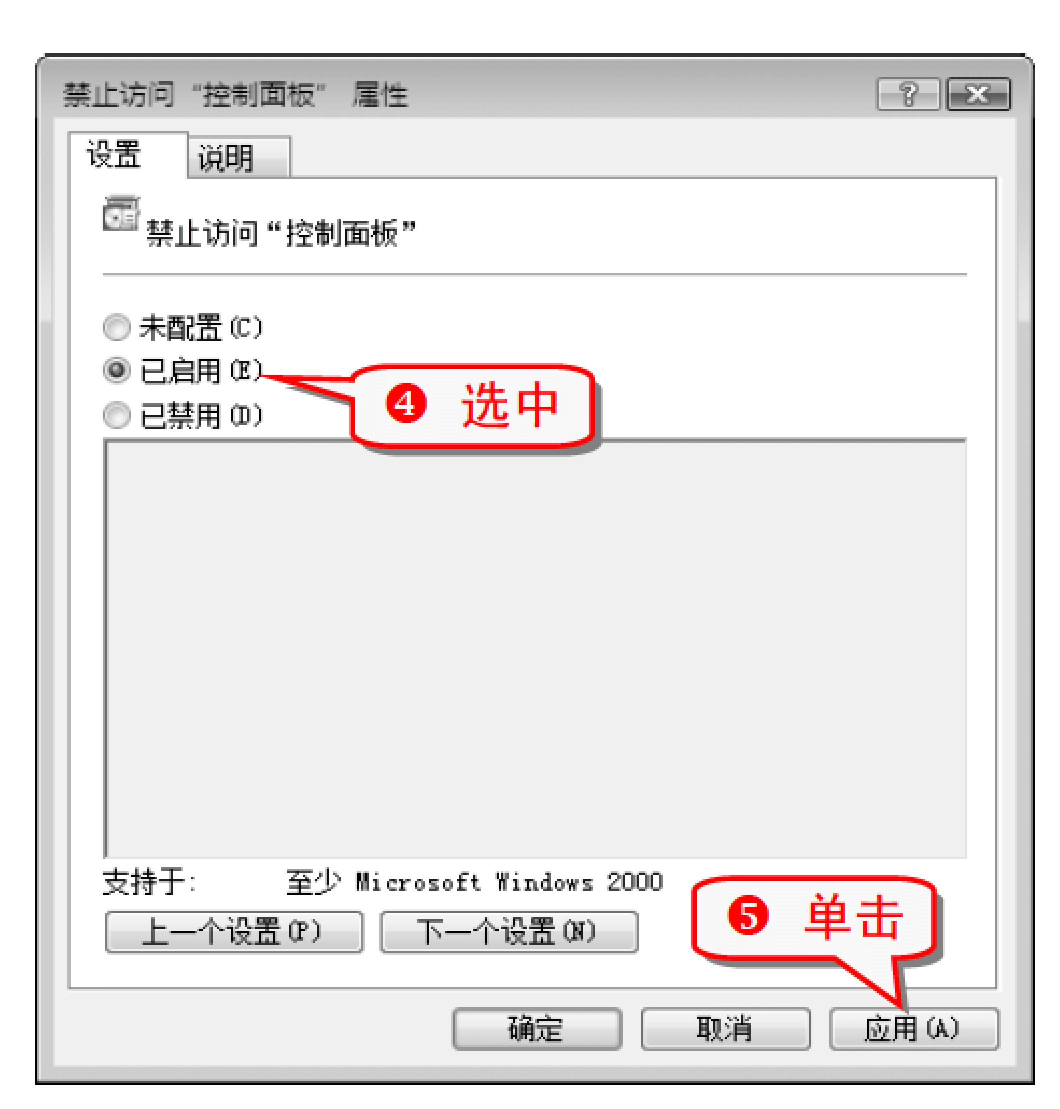
要撤销停用命令提示符，只要禁用“阻止访问命令提示符”策略就可以了。

技巧118 禁止访问控制面板

在控制面板中可以对电脑的大部分软件硬件进行设置和控制。为了防止黑客通过控制面板进行非法操作，有必要启用禁止访问控制面板功能。

❶ 打开组策略对象编辑器。



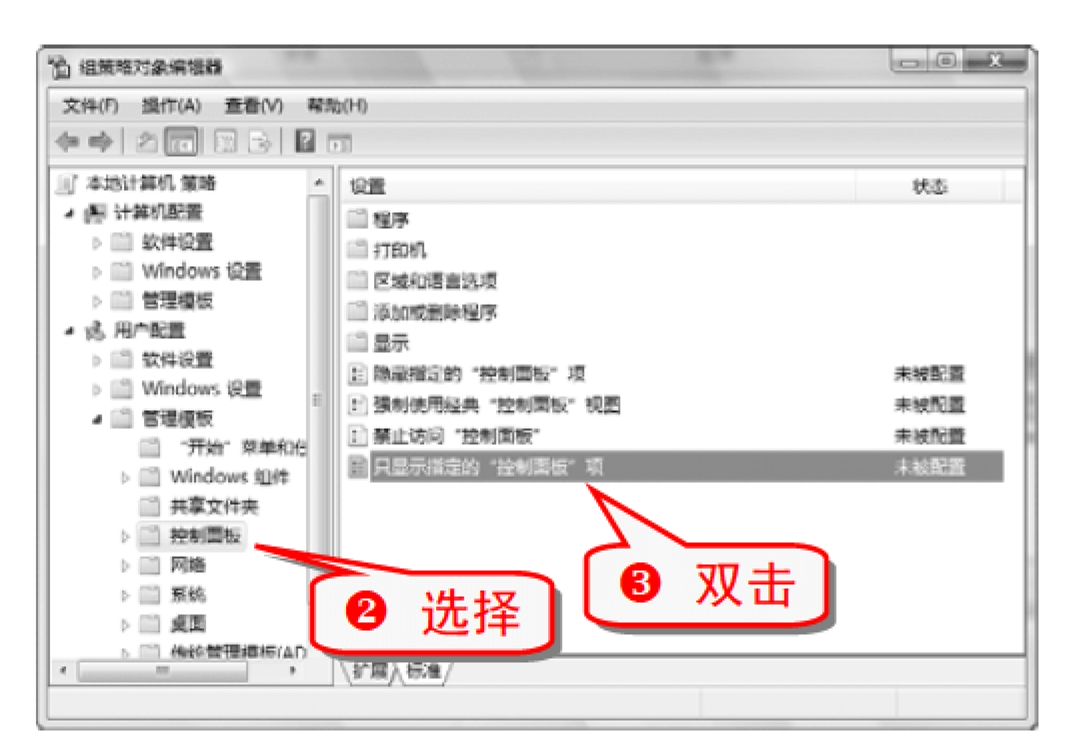


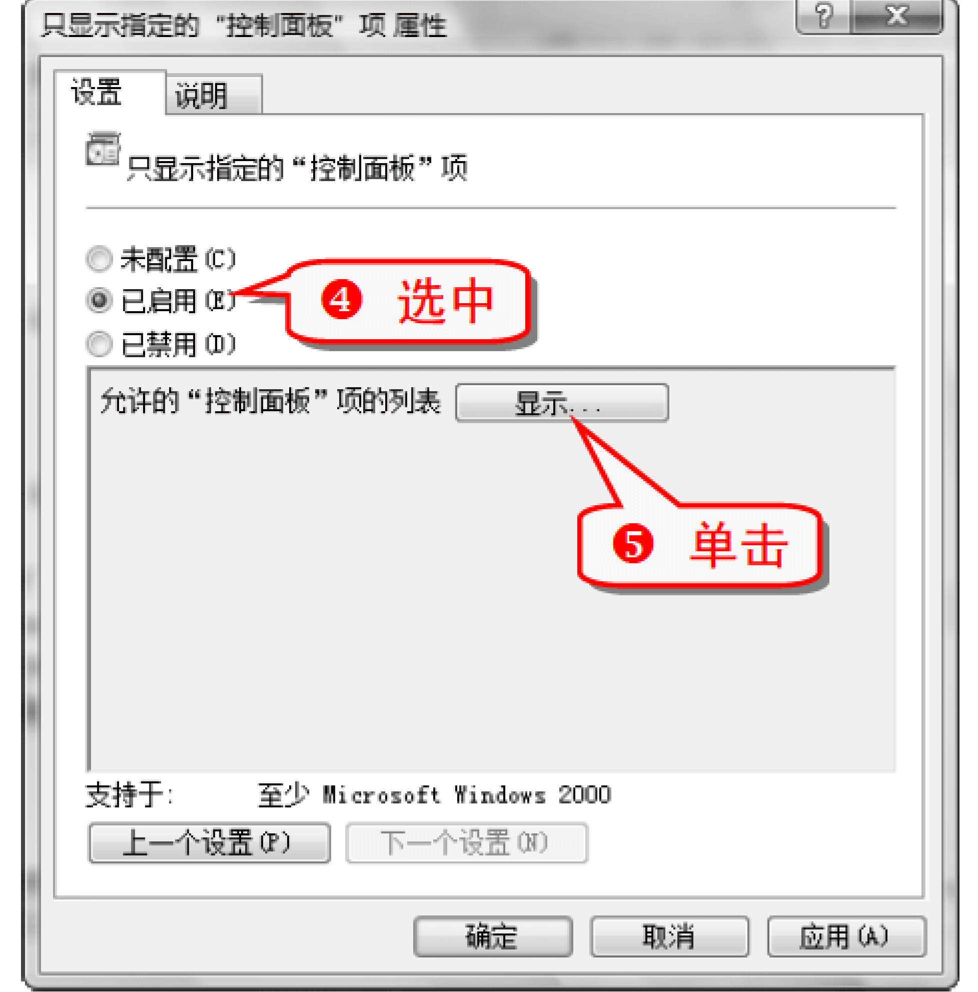
❻ 打开「开始」菜单可以发现，在菜单中没有“控制面板”选项。

技巧119 选择性地显示控制面板中的项

通过简单的几步设置可以让控制面板中只显示用户需要的项。

❶ 打开组策略对象编辑器。







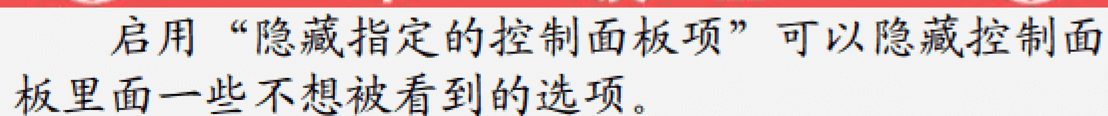






⑩ 打开“控制面板”窗口，“控制面板”窗口中只显示刚才选择的控制面板项。





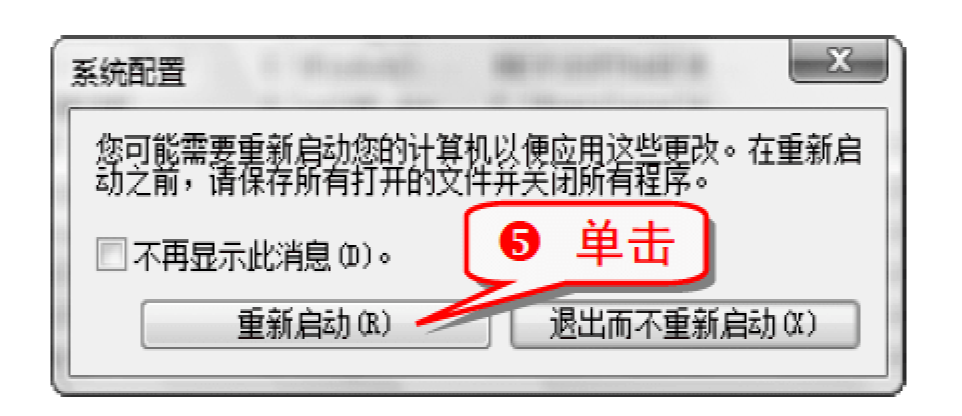
启用“隐藏指定的控制面板项”可以隐藏控制面板里面一些不想被看到的选项。

技巧120　禁用不需要的启动项

开机的时候系统会自动启动很多程序，严重影响开机速度，可用以下方法禁用程序，提高开机速度。

❶ 打开“运行”对话框，输入 msconfig 命令，弹出“系统配置”对话框。

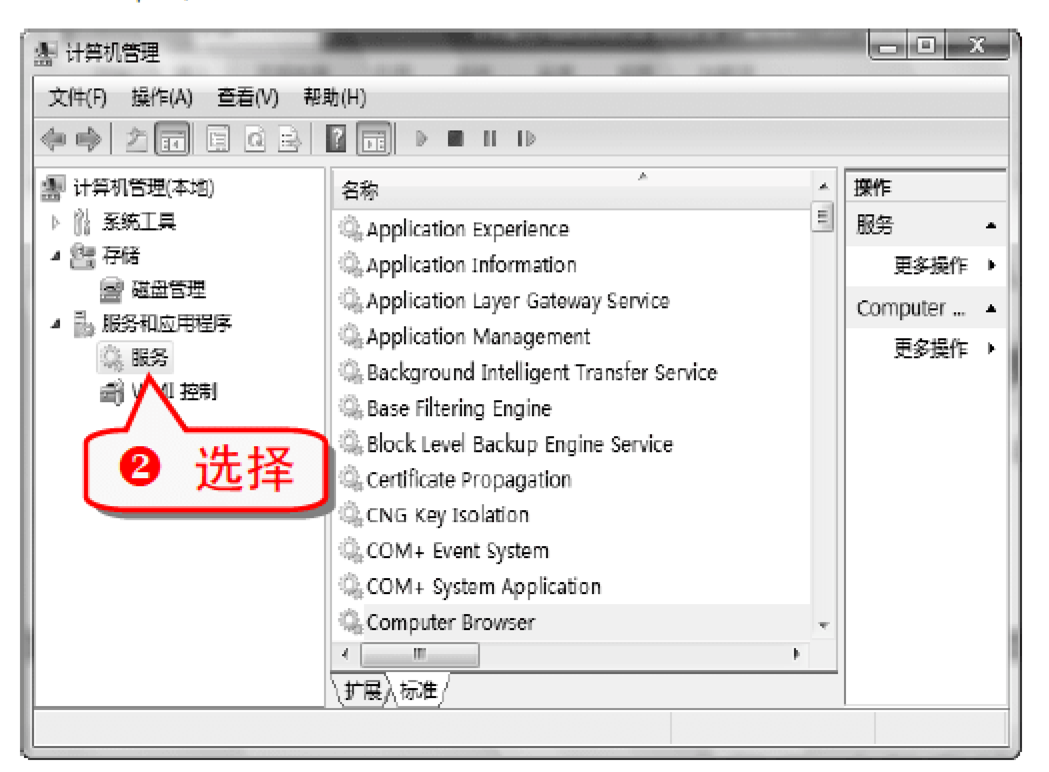




技巧121　禁用多余的服务组件

Windows Vista 启动的同时也启动了很多服务，有些服务是没有用的，有必要将其禁用。

❶ 右击“计算机”图标，在弹出的快捷菜单中选择“管理”命令。

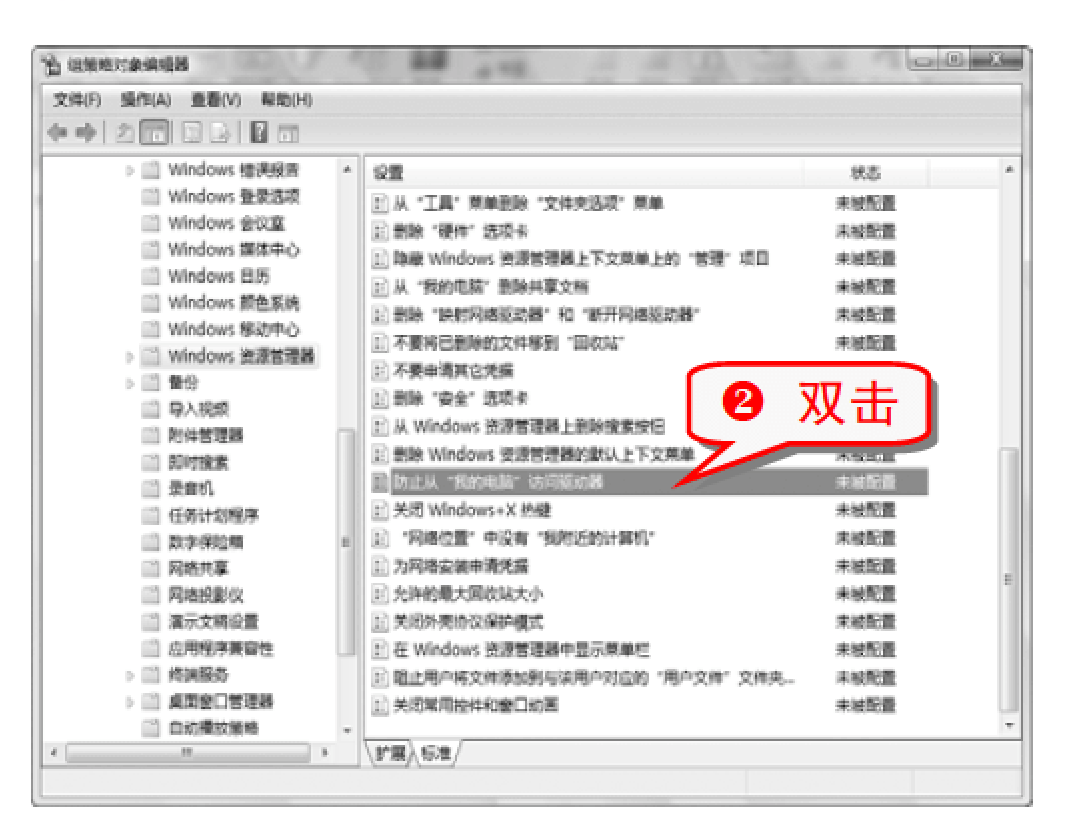


❸ 这样即可禁用不需要的服务组件。

技巧122　禁止从“计算机”界面访问驱动器

此策略可以禁止从“计算机”界面或是“资源管理器”界面访问所禁止的驱动器的内容。

❶ 打开组策略对象编辑器，展开“用户配置”→“管理模板”→“Windows 组件”→“Windows 资源管理器”选项。





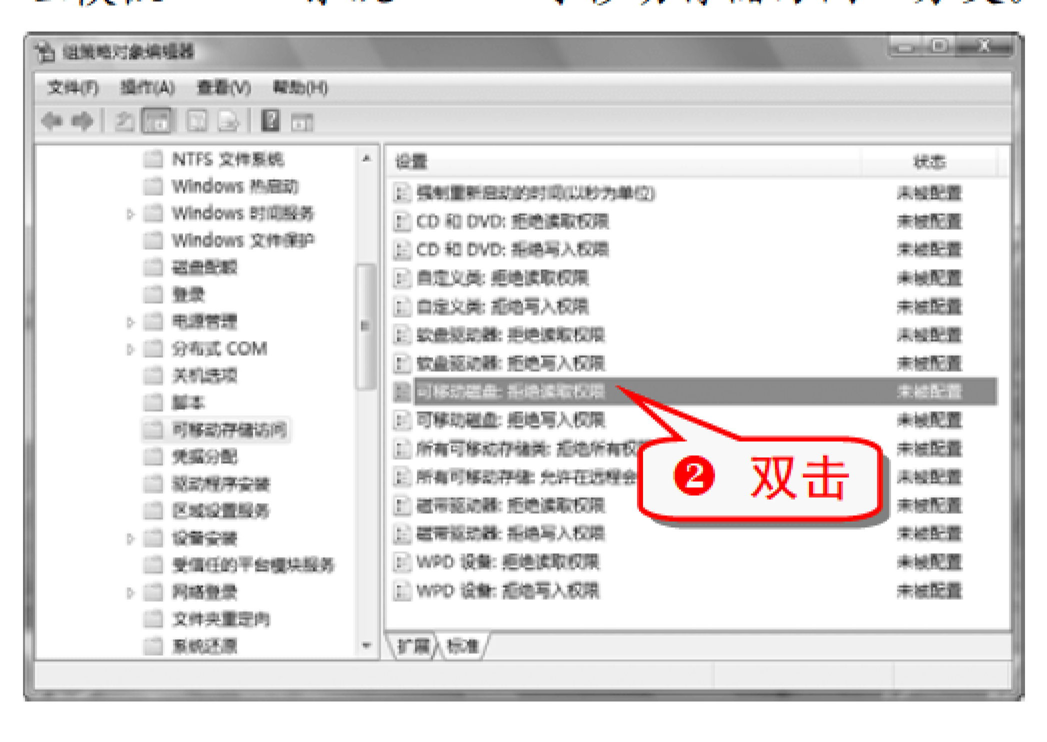
❻ 访问D盘时弹出"限制"警告框。



技巧123 禁用可移动磁盘的读取权限

禁用可移动磁盘的读取功能，可以防止可移动磁盘向电脑传播病毒。

❶ 打开组策略对象编辑器，展开"计算机配置"→"管理模板"→"系统"→"可移动存储访问"分支。





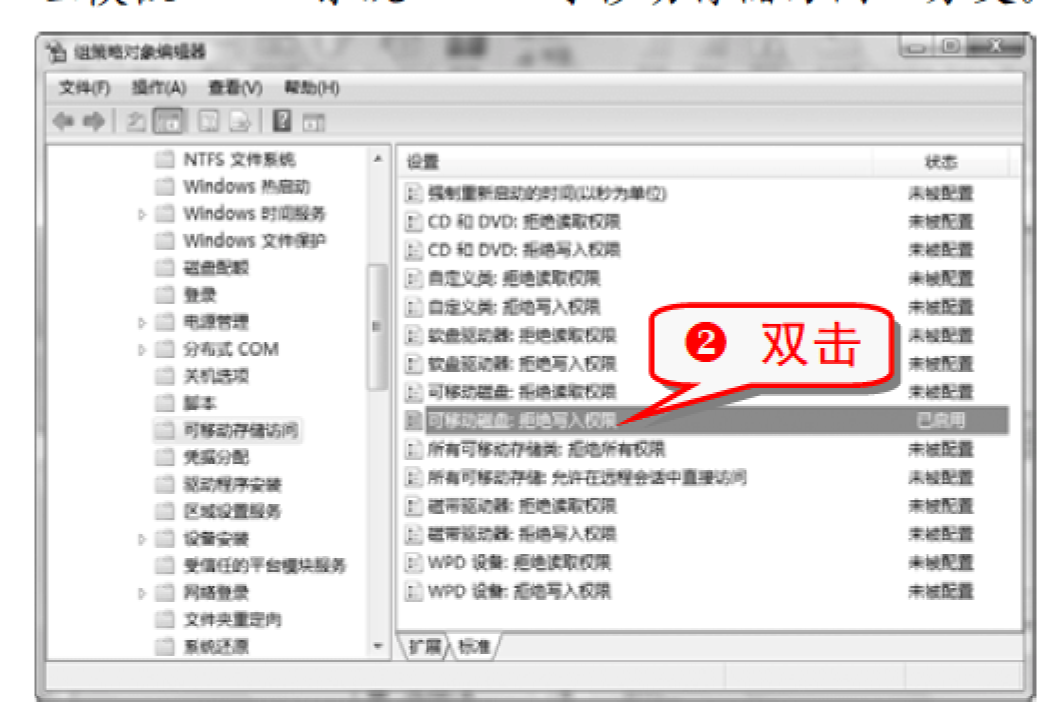
❺ 访问可移动磁盘时，弹出"位置不可用"警告框。



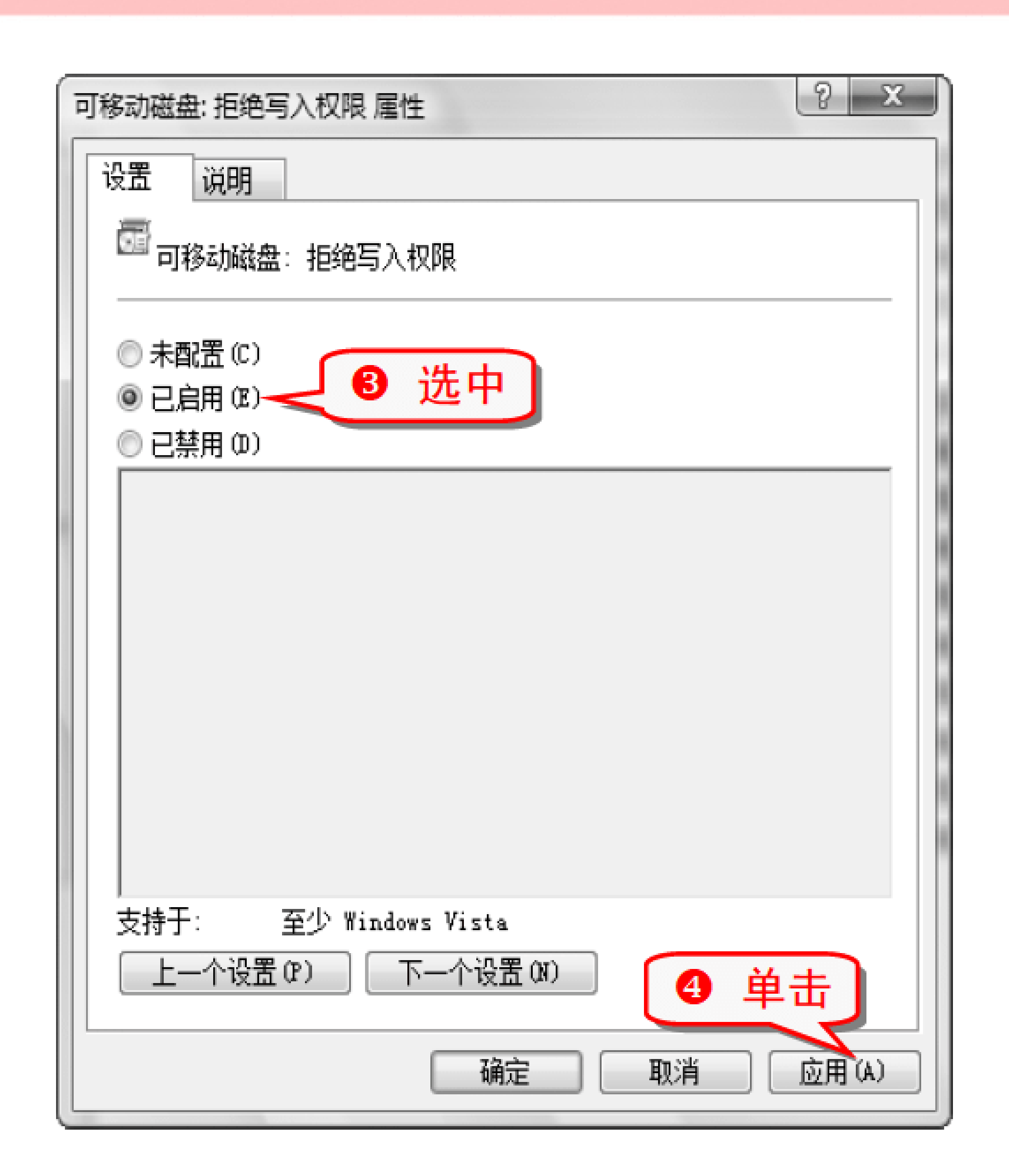
技巧124 禁用可移动磁盘的写入权限

禁用可移动磁盘的写入功能，可以防止从电脑传播病毒到移动硬盘上。

❶ 打开组策略对象编辑器，展开"计算机配置"→"管理模板"→"系统"→"可移动存储访问"分支。







❺ 往可移动磁盘写入内容时，弹出“目标文件夹访问被拒绝”提示框。

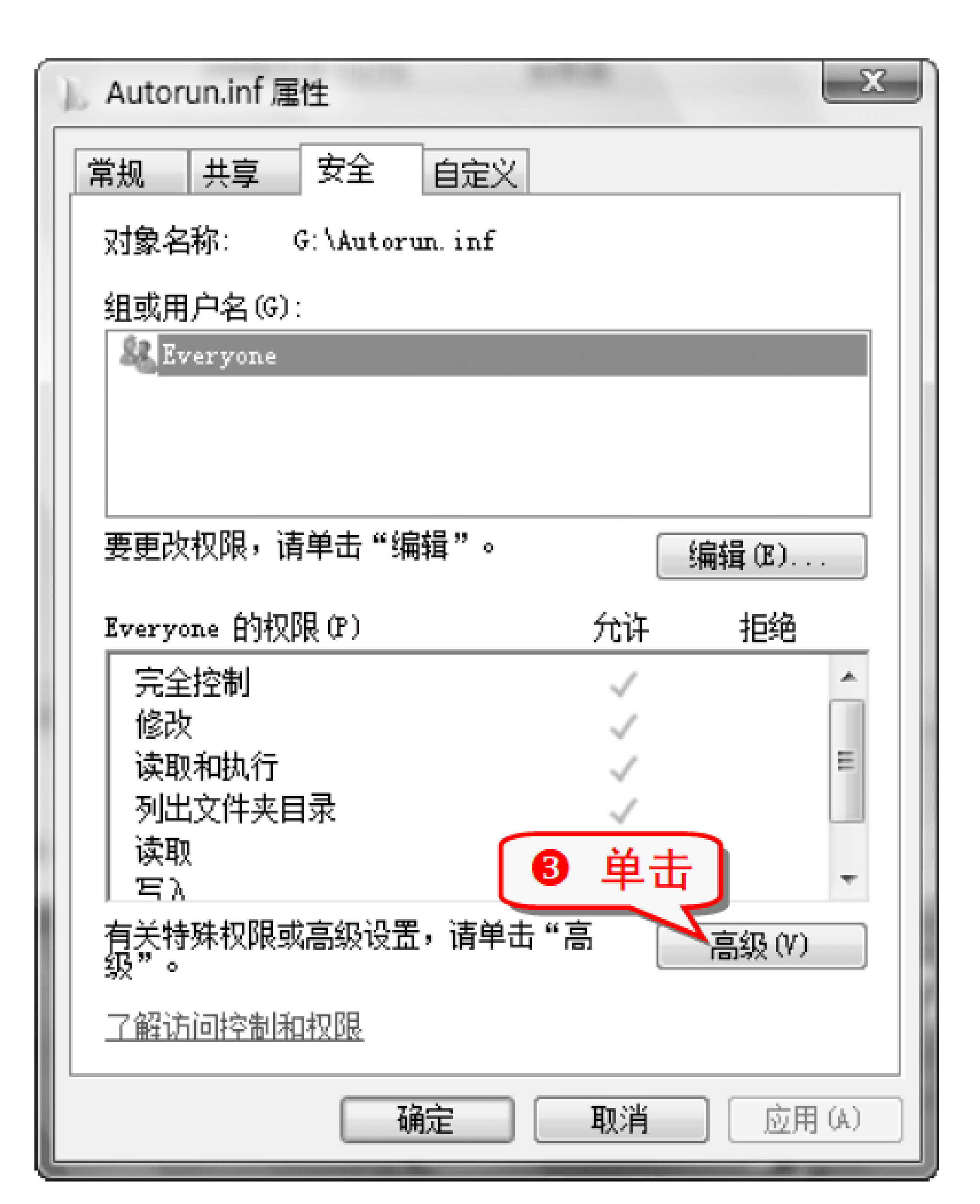


技巧125　在 Windows Vista 中打造安全 U 盘

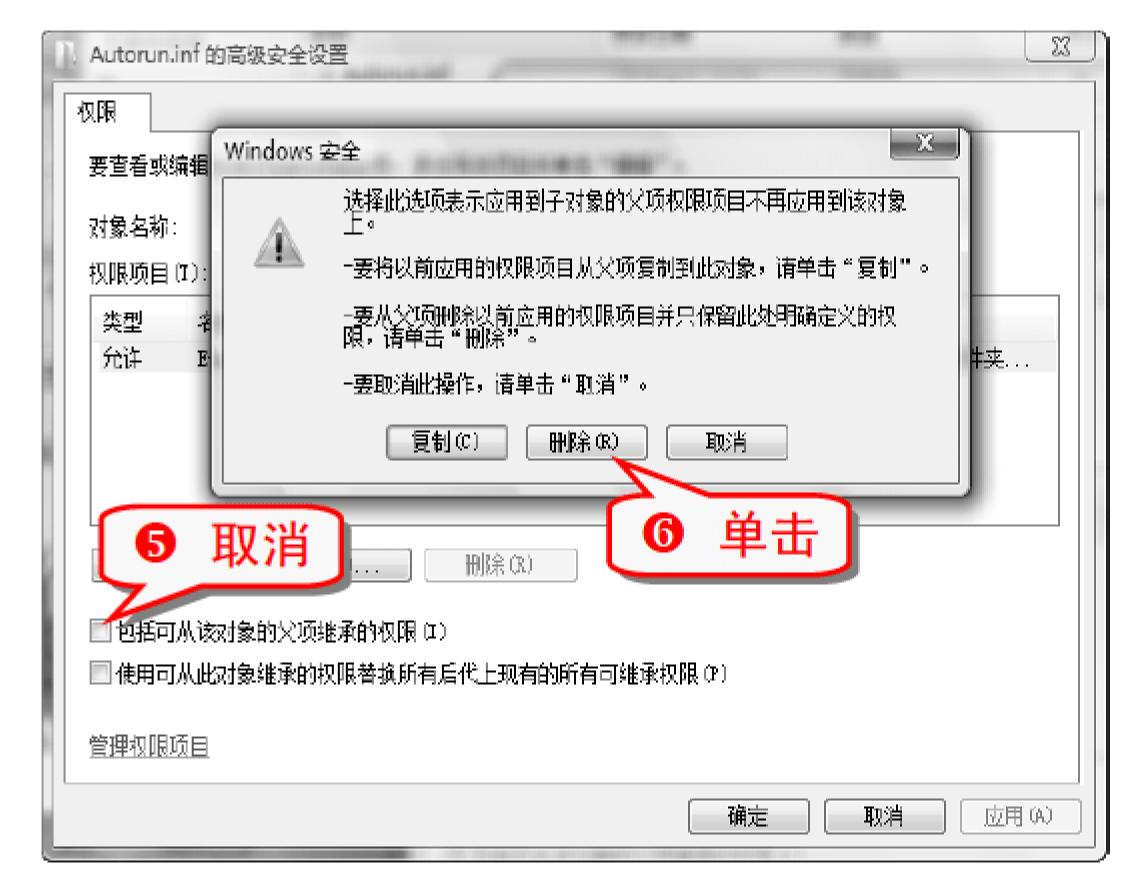
在 Windows Vista 中对 U 盘进行简单的设置，可以很好地防御 U 盘 autorun 病毒。

❶ 将 U 盘格式化为 NTFS 格式。

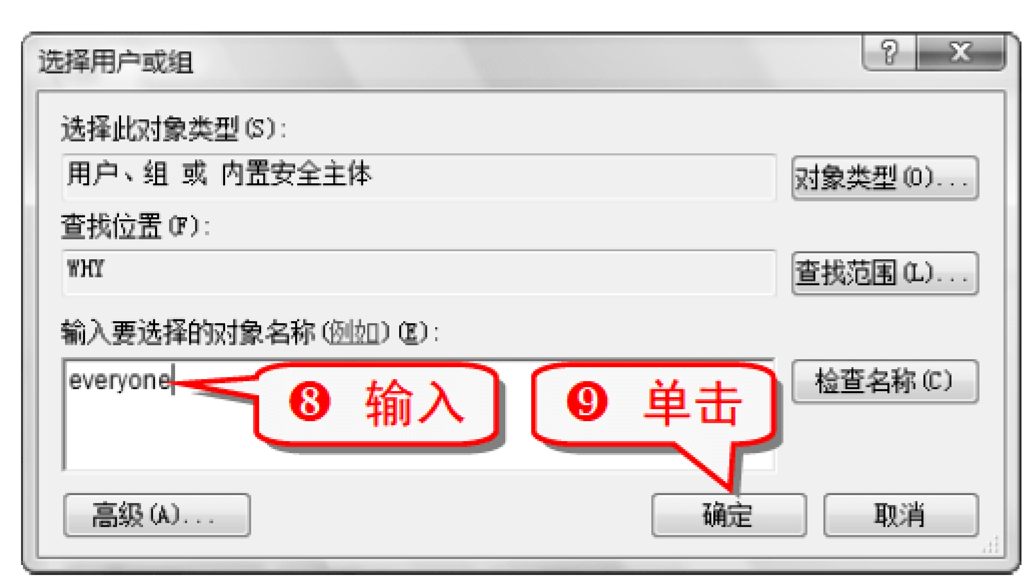
❷ 在 U 盘中新建一个文件夹，重命名为 Autorun.inf，右击 Autorun.inf 文件夹，在弹出的快捷菜单中选择“属性”命令。

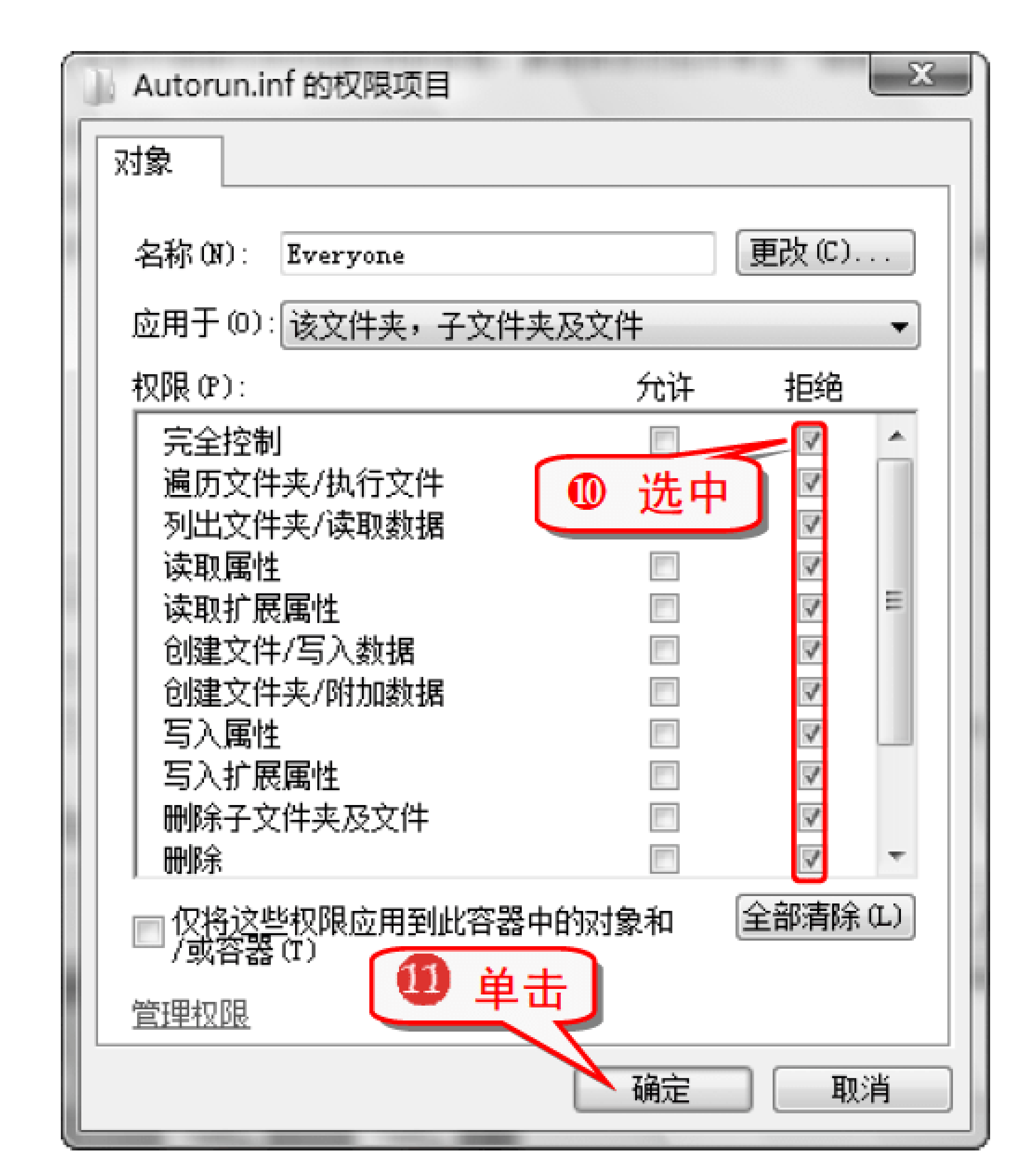












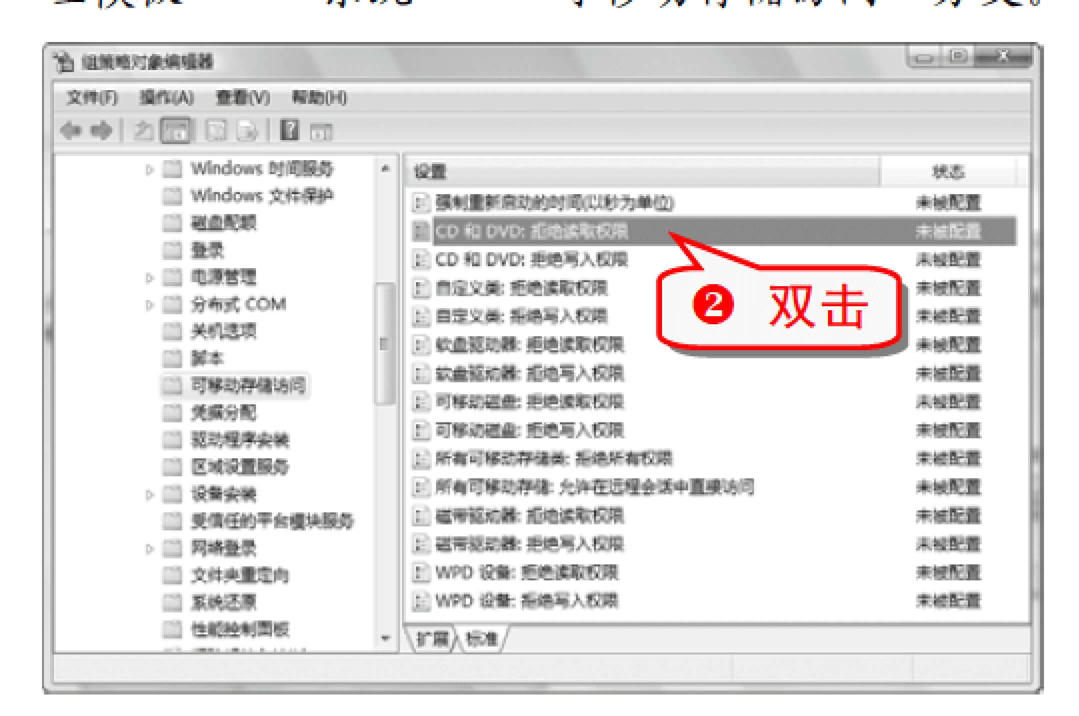
注 意 事 项

经过上述设置 autorun.inf 文件夹权限为不可写、不可删除以及不可改名。即使U盘感染了 autorun 病毒，病毒也不会自动运行。

技巧126 禁用 DVD 驱动器的读取权限

禁用 DVD 驱动器的读取功能，可以防止从光盘安装非法软件到电脑上。

❶ 打开组策略对象编辑器，展开"计算机配置"→"管理模板"→"系统"→"可移动存储访问"分支。





❺ 访问光盘时，弹出"找不到应用程序"的警告框。



技巧127 禁止使用*.reg 文件

.reg 文件一般为注册表备份文件，将其禁止，可以很好地防止黑客使用此类文件对注册表进行恶意修改，其默认功能是直接导入注册表，禁止使用.reg 文件还可以很好地防止用户误操作。

❶ 打开注册表编辑器，展开 HKEY_LOC AL_MACHINE\



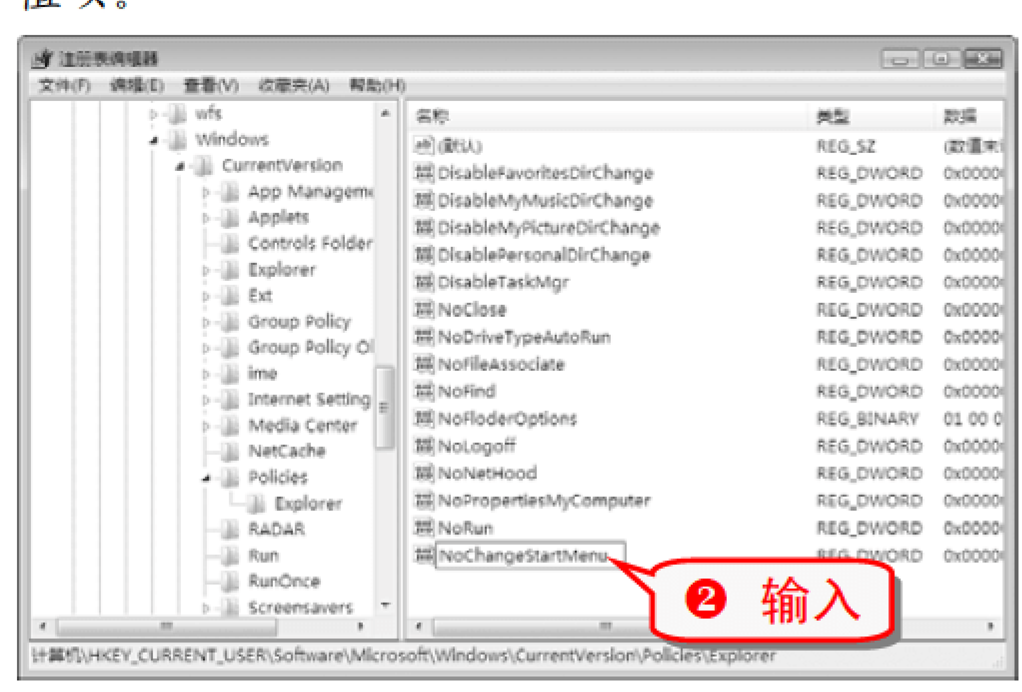
SOFTWARE\Classes\.reg 分支。

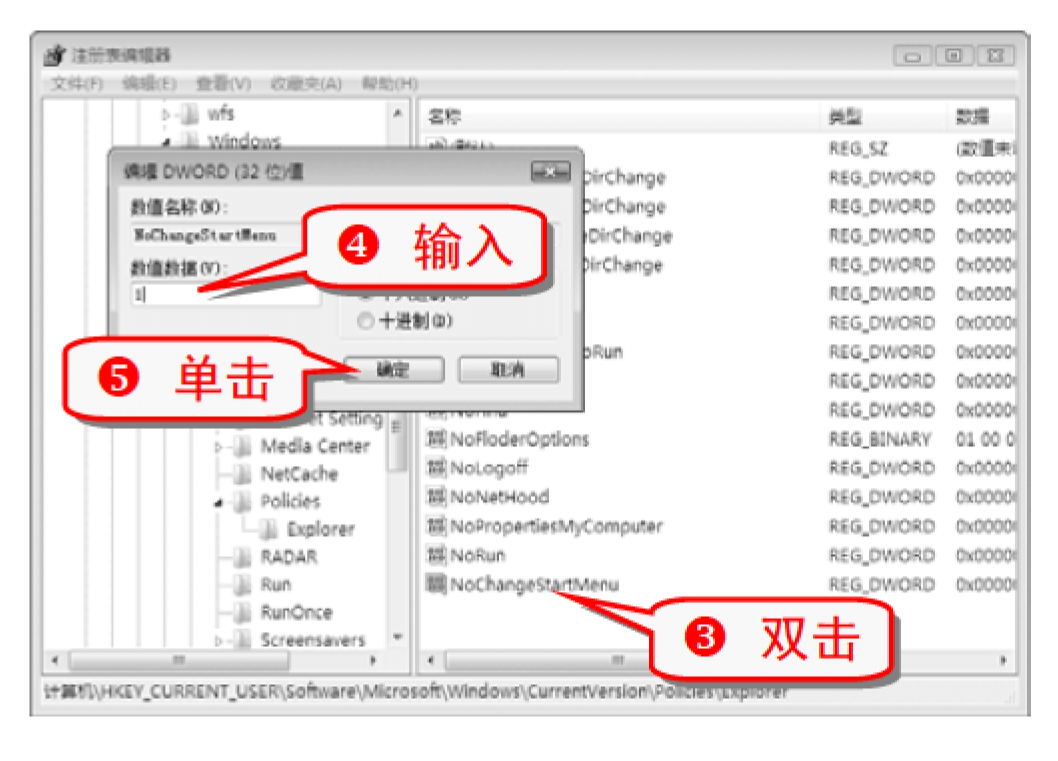


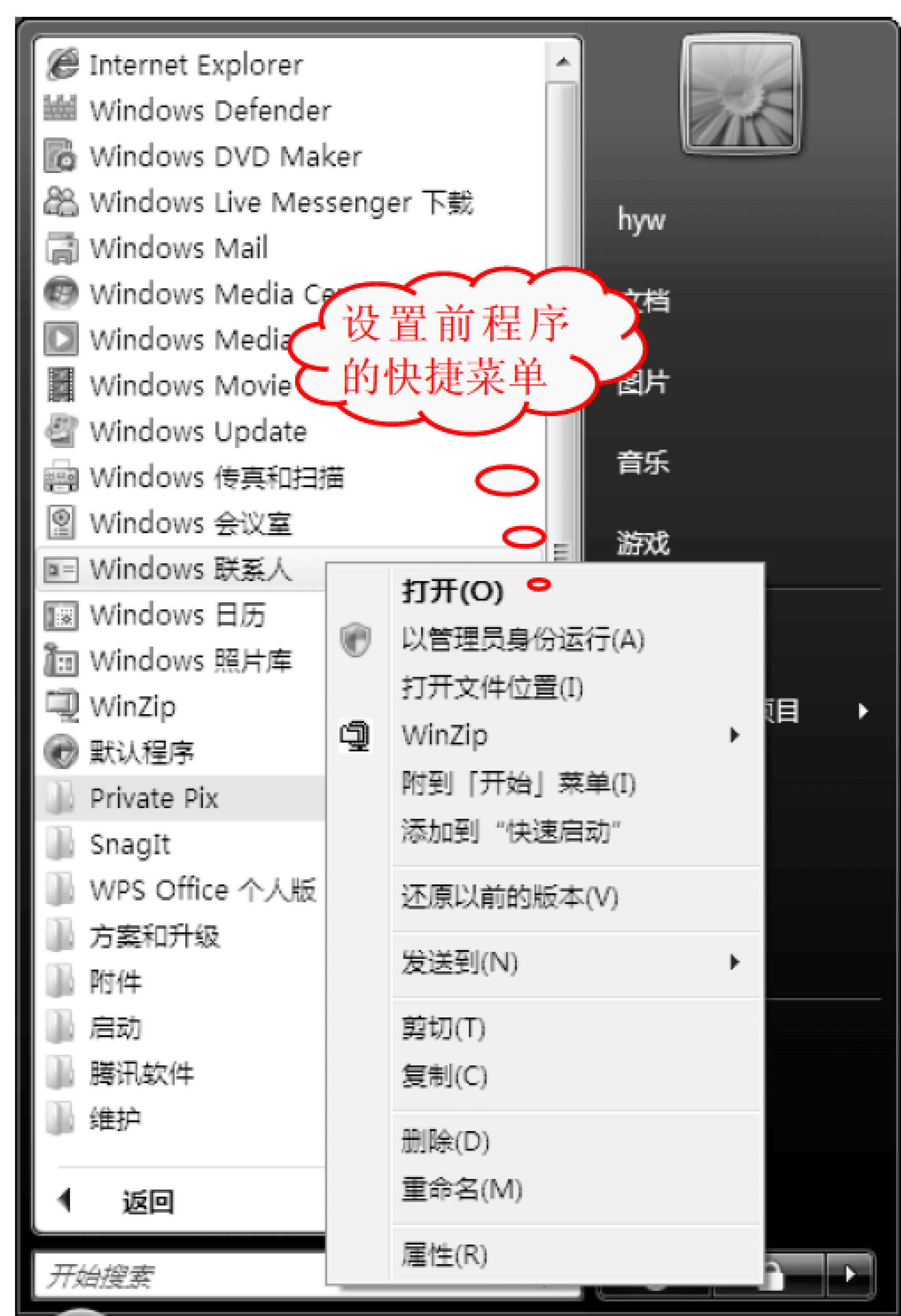
技巧128　禁止修改「开始」菜单

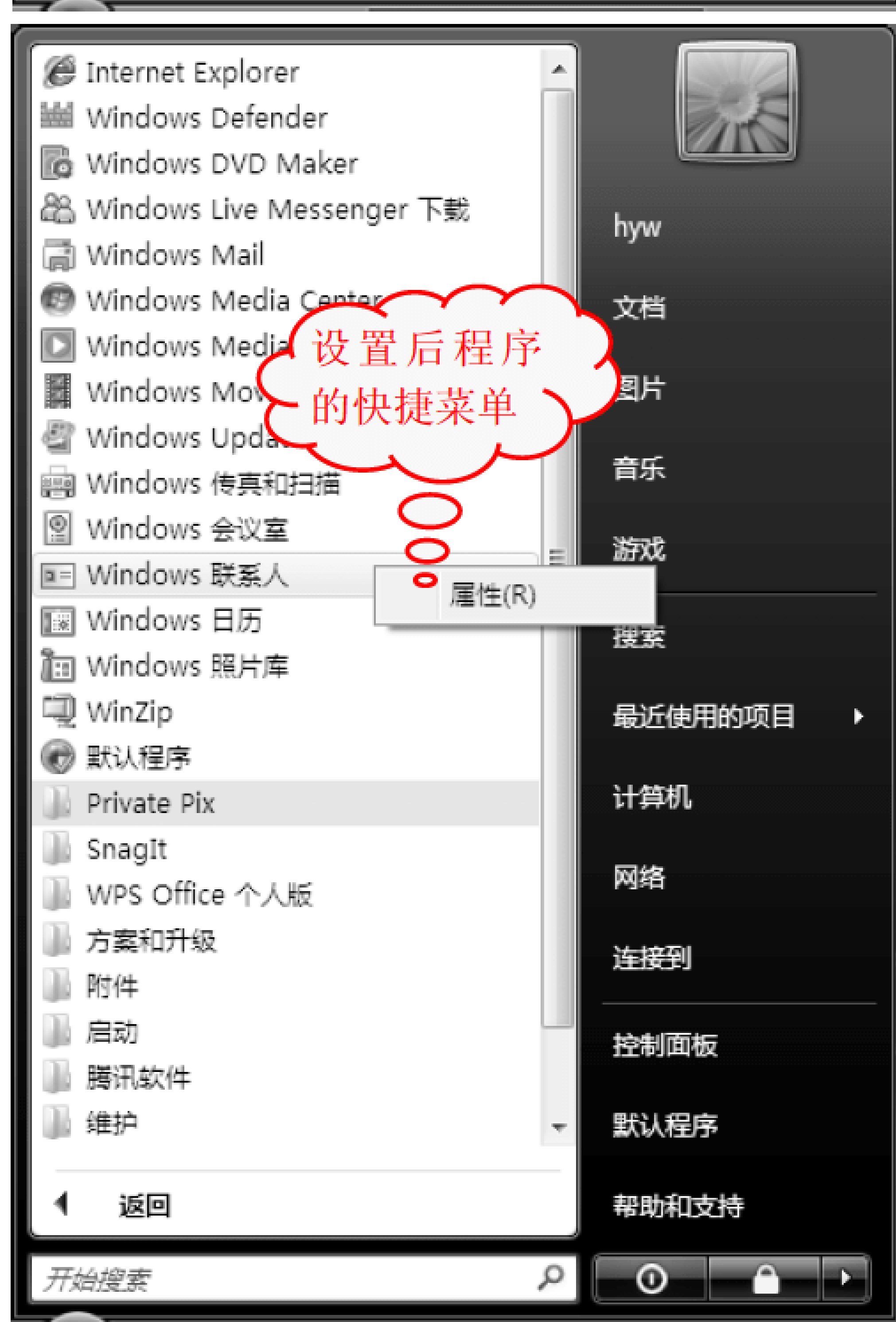
正常情况下，用户可以通过右击的方式修改「开始」菜单的内容，如果不想让其他人修改「开始」菜单的内容，可以通过修改注册表来实现。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支，新建一个类型为 DWORD(32 位)的键值项。









注 意 事 项

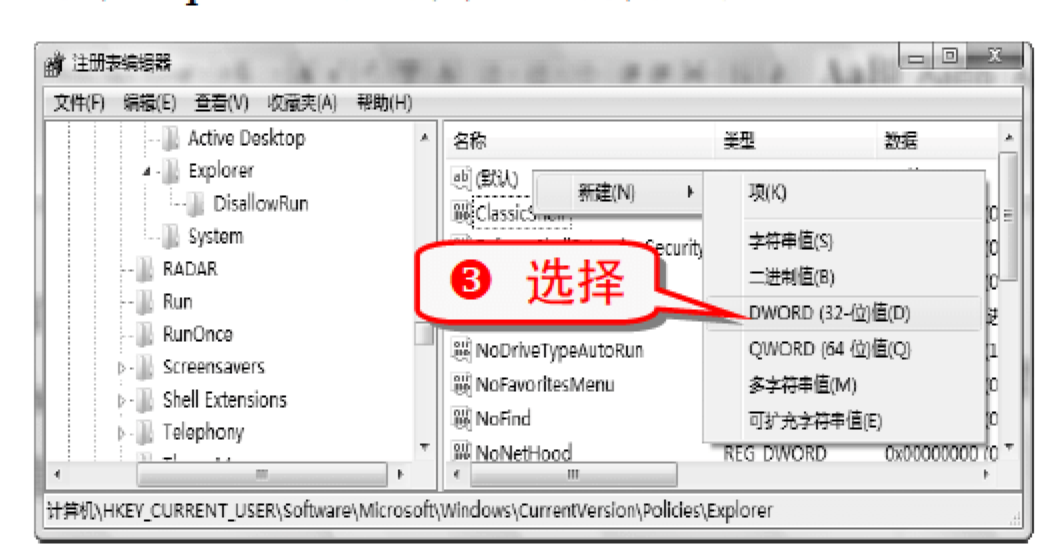
将 NoChangeStartMenu 的键值设置为 0，则允许修改「开始」菜单。设置在注销或重新启动后生效。

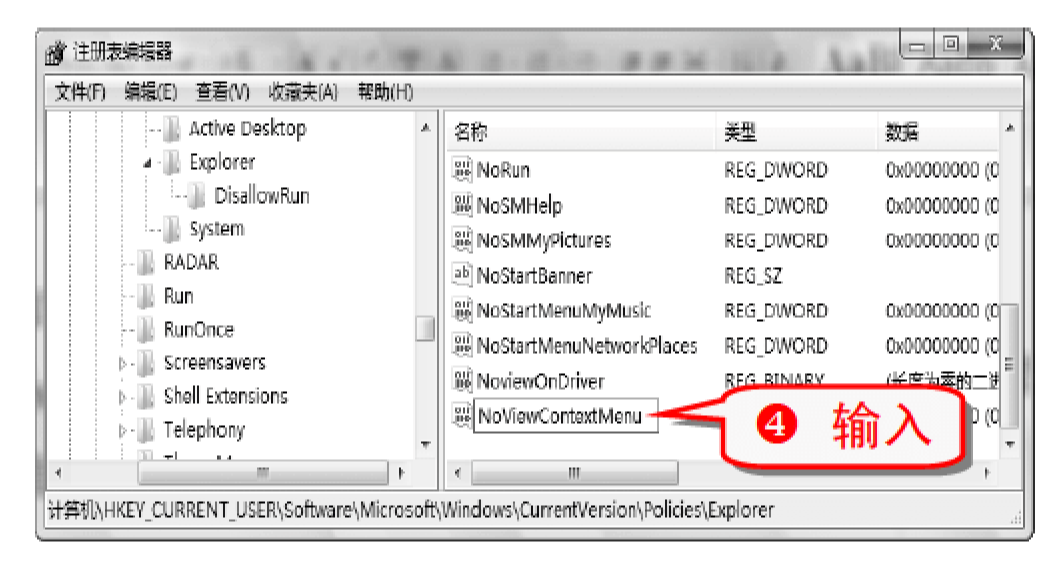
技巧129 禁止在资源管理器中使用右键

禁止在资源管理器中使用右键，可以防止对资源管理器进行非法修改。

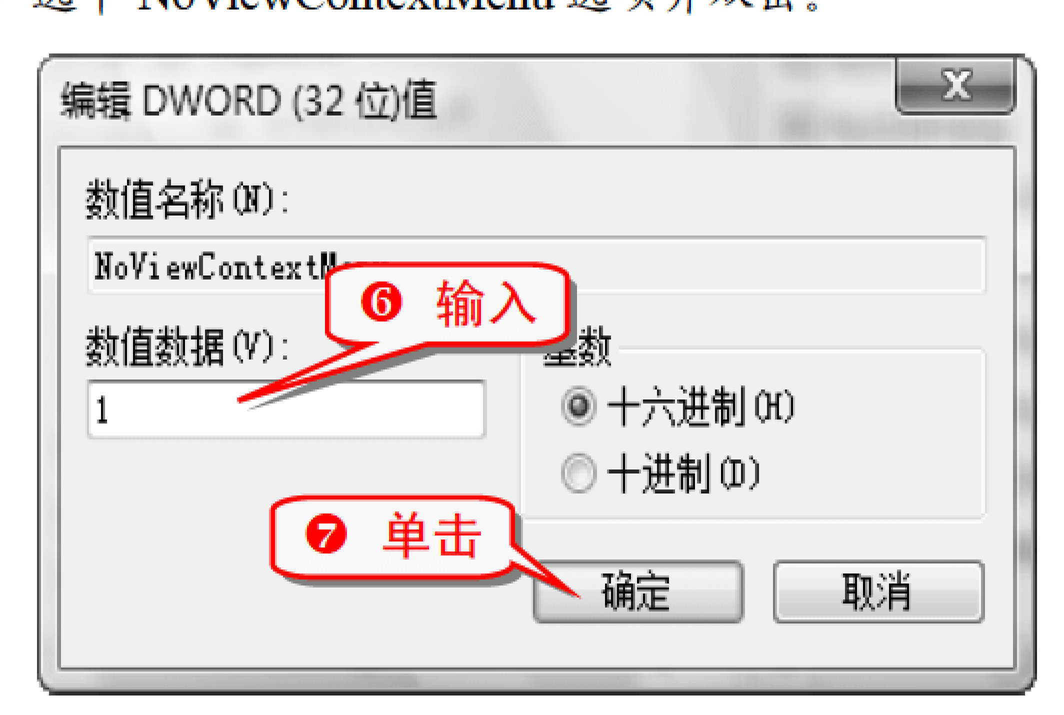
❶ 打开注册表编辑器，展开 HKEY_CURR ENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支。

❷ 选择 Explorer 选项并在右边窗格的空白处右击。





❺ 选中 NoViewContextMenu 选项并双击。

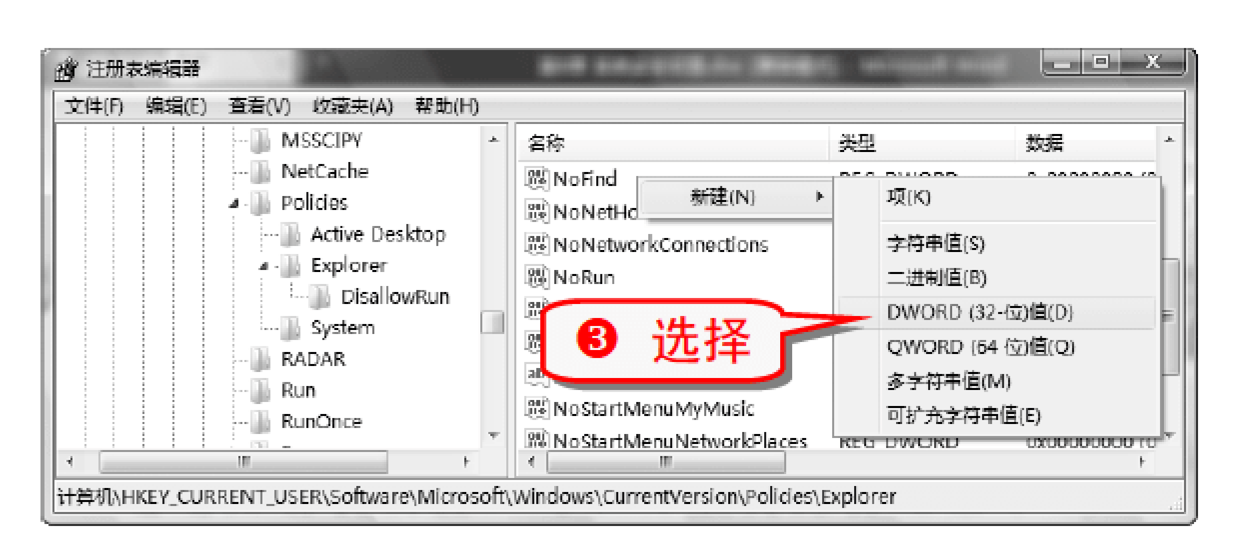


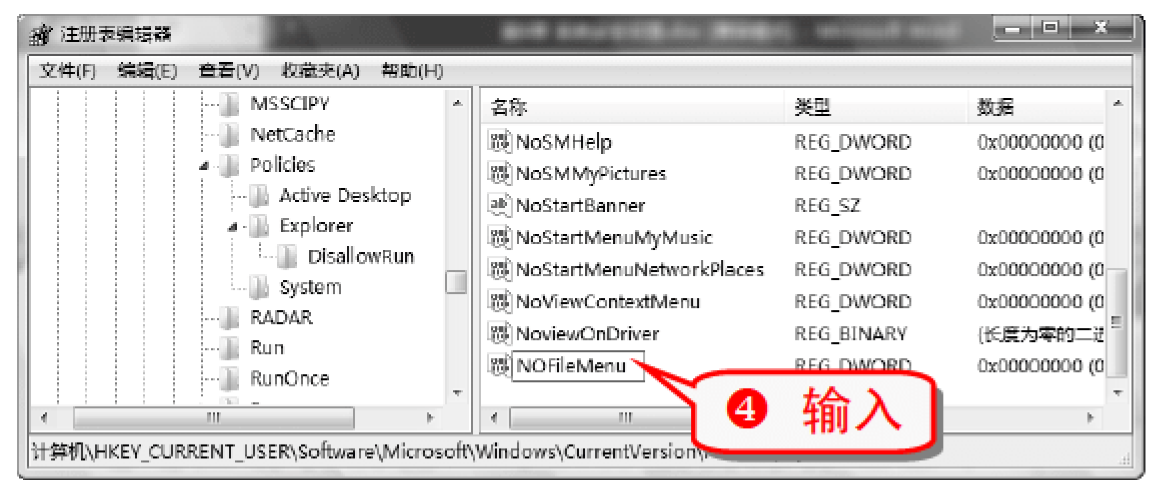
技巧130 屏蔽 Windows 资源管理器中的文件菜单

文件菜单可以打开和管理文件，屏蔽 Windows 资源管理器中的文件菜单可以有效地管理文件系统。

❶ 打开注册表编辑器，展开 HKEY_CURR ENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 分支。

❷ 选择 Explorer 选项并在右边窗格中的空白处右击。





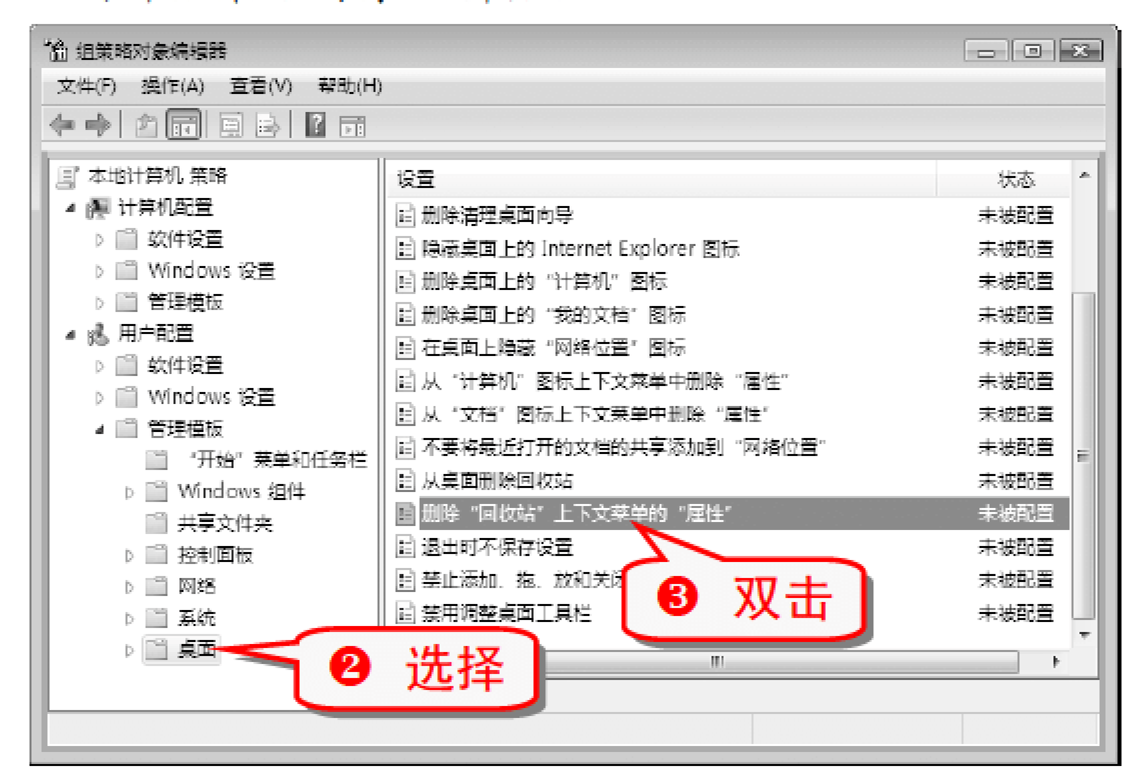
❺ 选中 NoFileMenu 选项并双击。



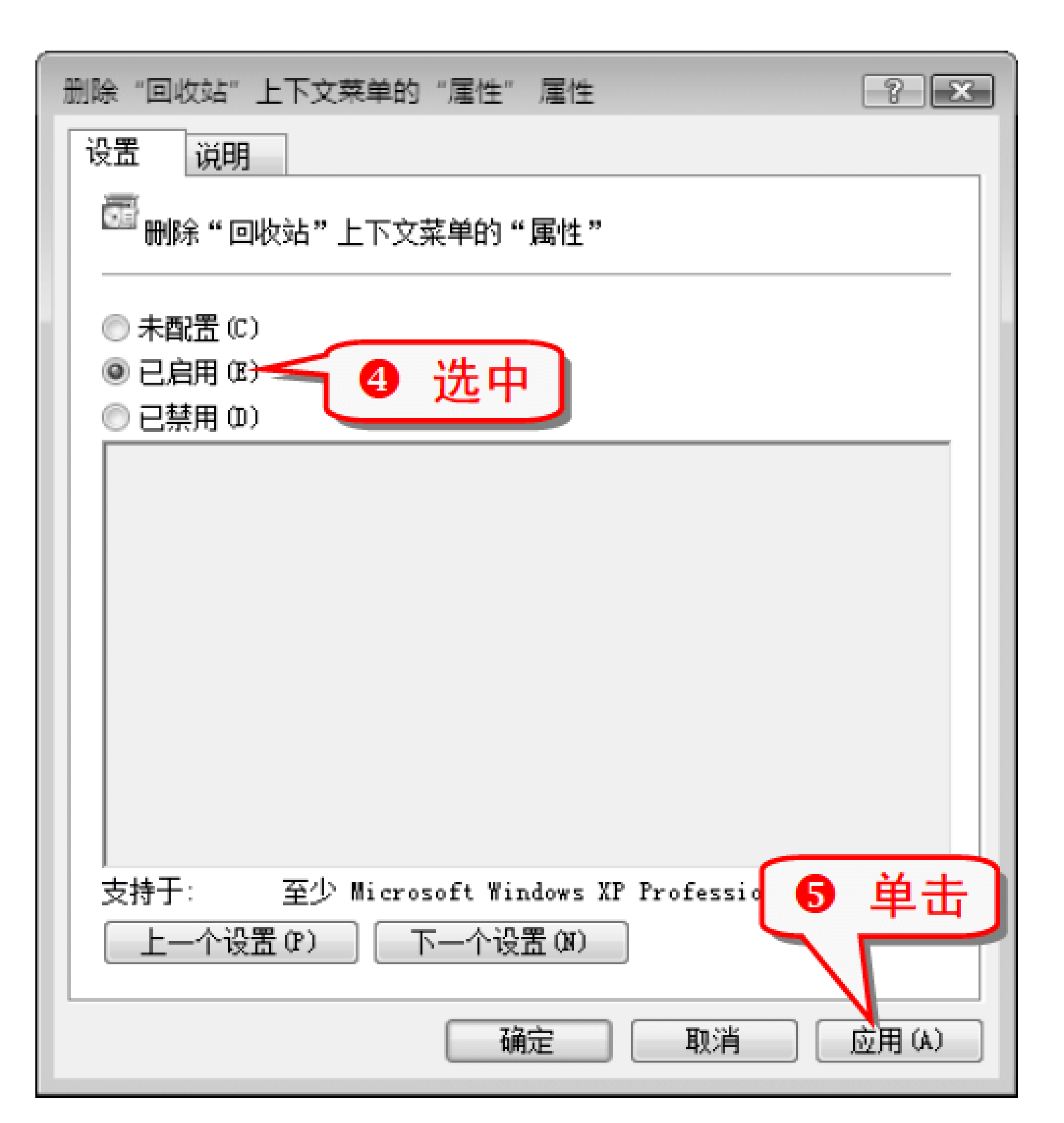
技巧131 从回收站的快捷菜单中删除“属性”选项

在右击“回收站”图标弹出的快捷菜单中，选择“属性”命令可以设置被删除文件的处理方式。删除“属性”选项，可以防止别人更改被删除文件的处理方式。

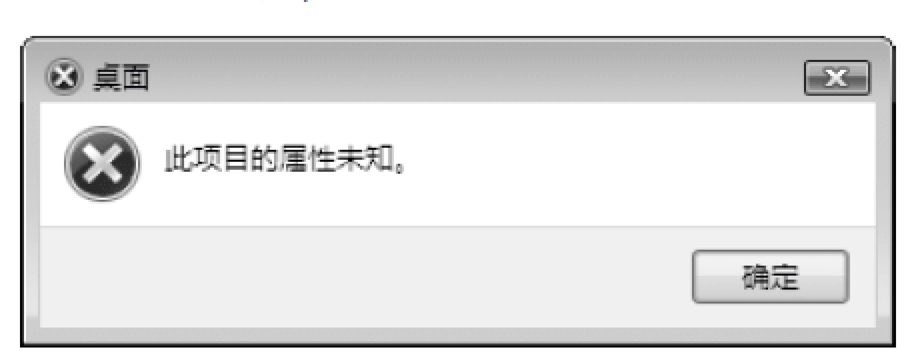
❶ 打开组策略对象编辑器。







❻ 右击回收站图标，在弹出的快捷菜单中选择“属性”命令，出现以下警告框。



技巧132　改变“安装/卸载”列表中的内容

在安装软件时，系统通常会自动将安装的程序添加到“安装/卸载”列表中，以便查看程序和卸载程序。通过修改注册表可以使安装的程序不被添加到列表中，可以防止误操作或者被发现。

❶ 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall 分支。

❷ 选择需要删除的程序，例如删除 360 安全卫士软件，并右击。



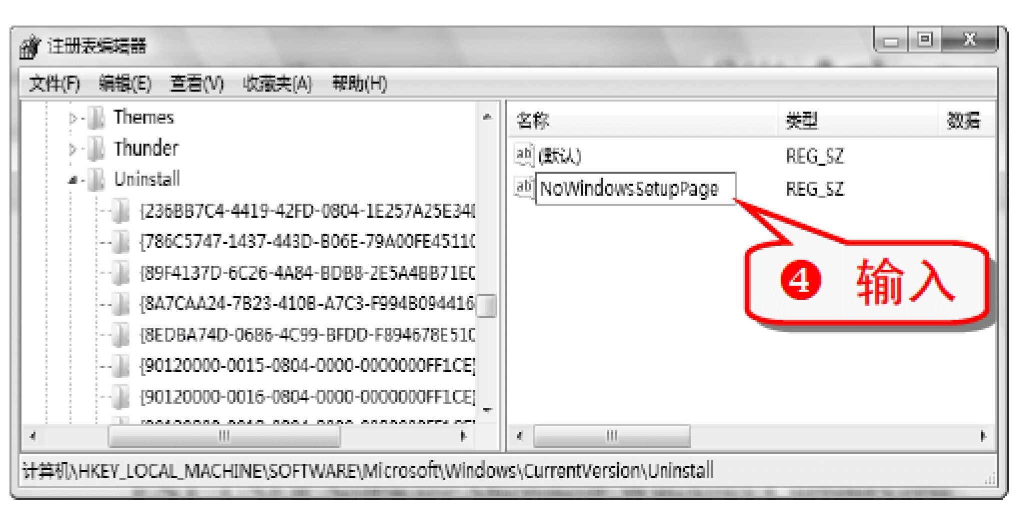
技巧133　隐藏“添加/删除组件”选项

在 Windows 系统中有一个“添加/删除组件”的功能，隐藏“添加/删除组件”选项，可以防止程序不被随意卸载。

❶ 打开注册表编辑器，展开 HKEY_CURR ENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall 分支。

❷ 选择 Uninstall 选项并在右边窗格的空白处右击。





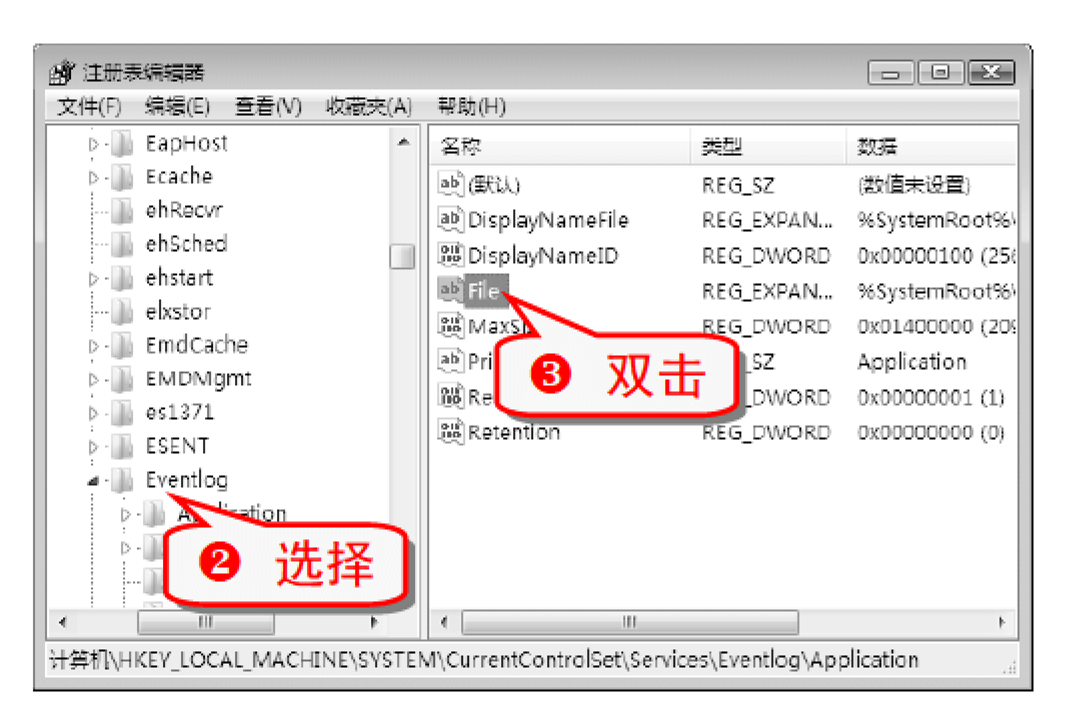
❺ 选中 NoWindowsSetupPage 选项并双击。



技巧134　改变日志文件默认路径

改变日志文件的默认存储路径是保护日志文件的好方法。

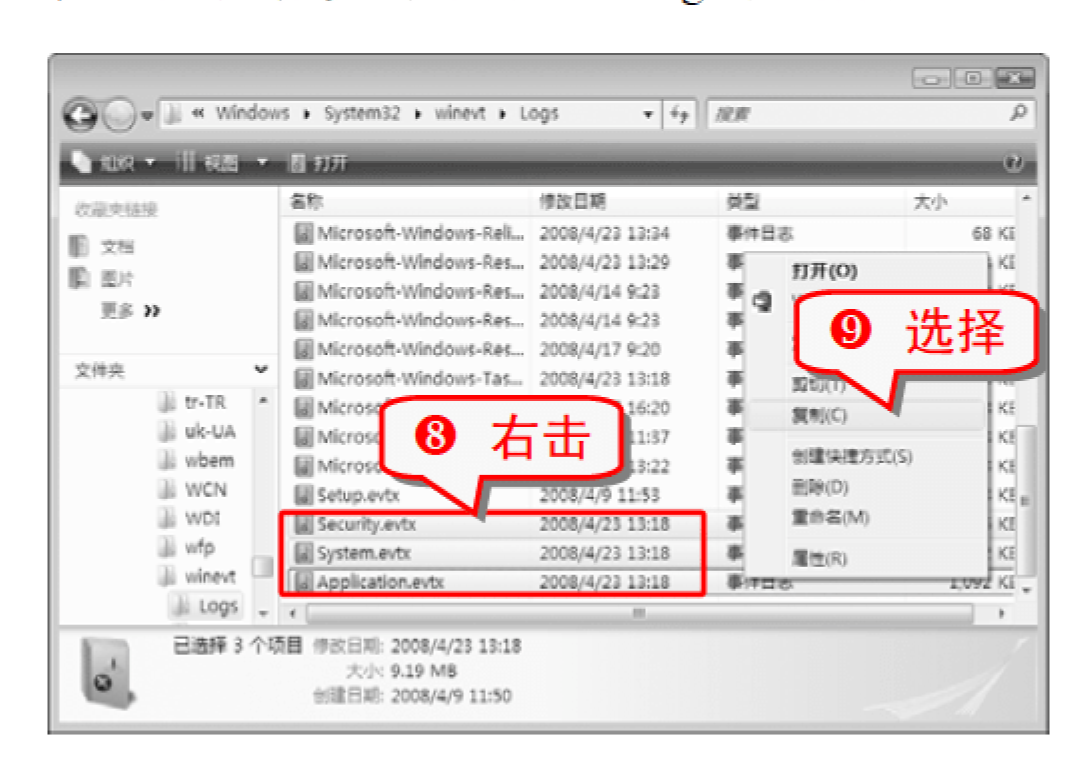
❶ 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Services\Eventlog 分支。

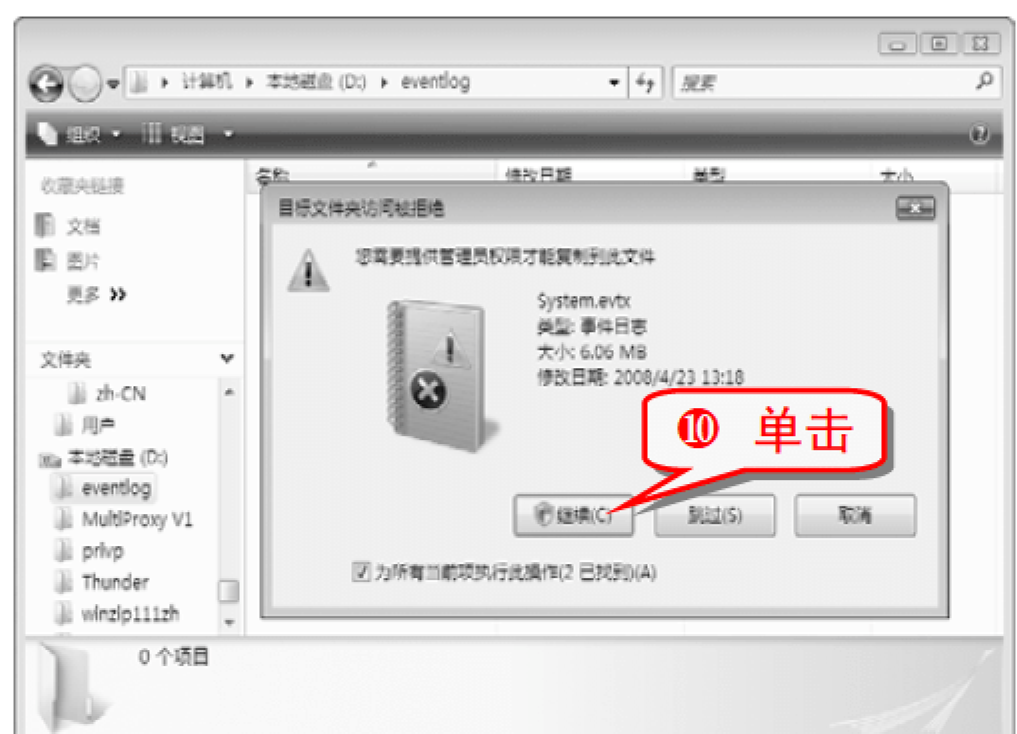




❻ 选择Eventlog选项下的Security和System子键进行同样的修改，Security的File值改为d:\eventlog\Security.evtx，System的File值改为d:\eventlog\System.evtx。

❼ 在D盘下新建一个名为eventlog的文件夹。







设置在注销或重新启动电脑后才能生效。

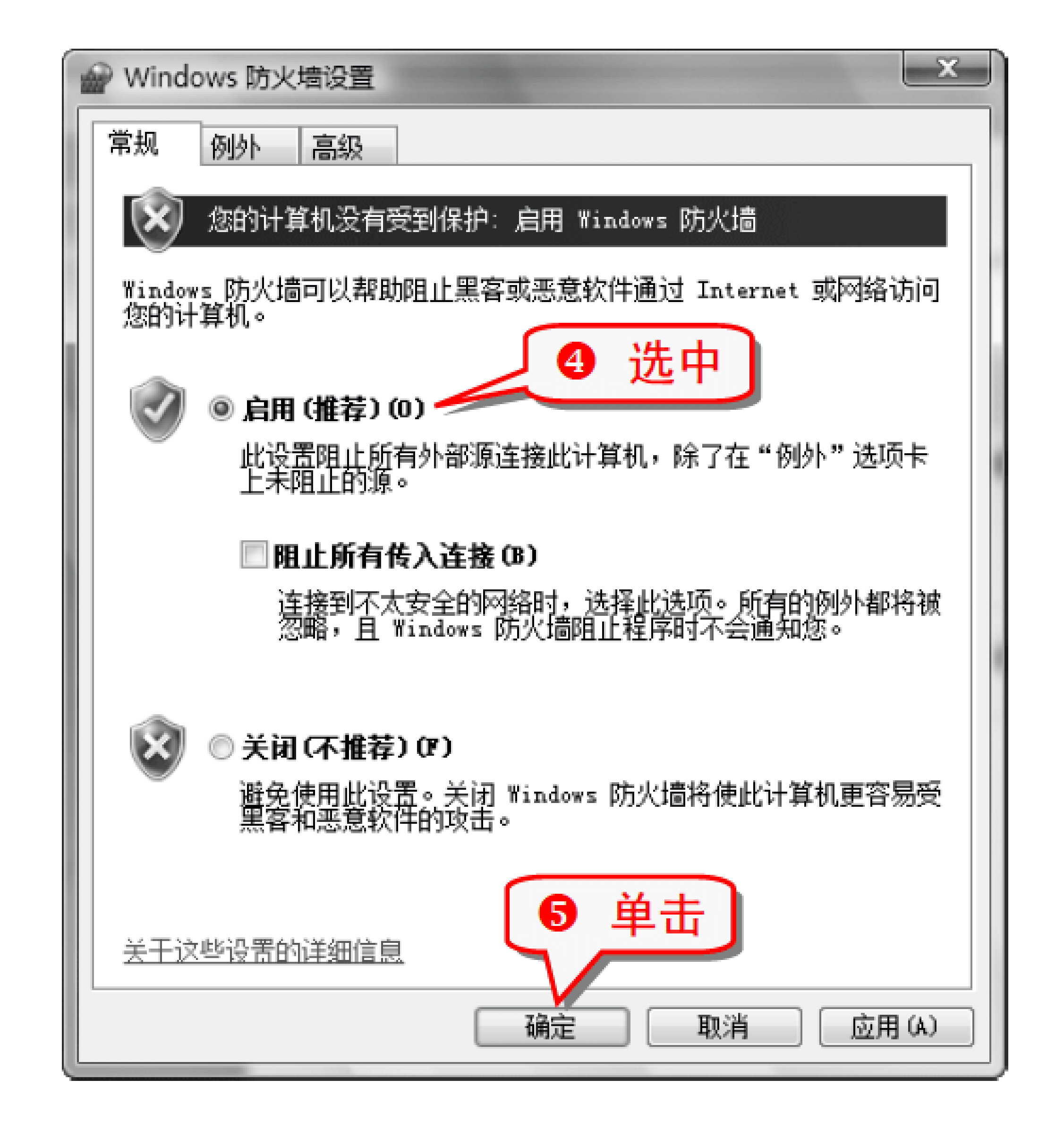
技巧135 启用Windows Vista自带防火墙

Windows Vista有一款自带的防火墙，能增加系统的安全性。

❶ 选择“开始”→“控制面板”命令。





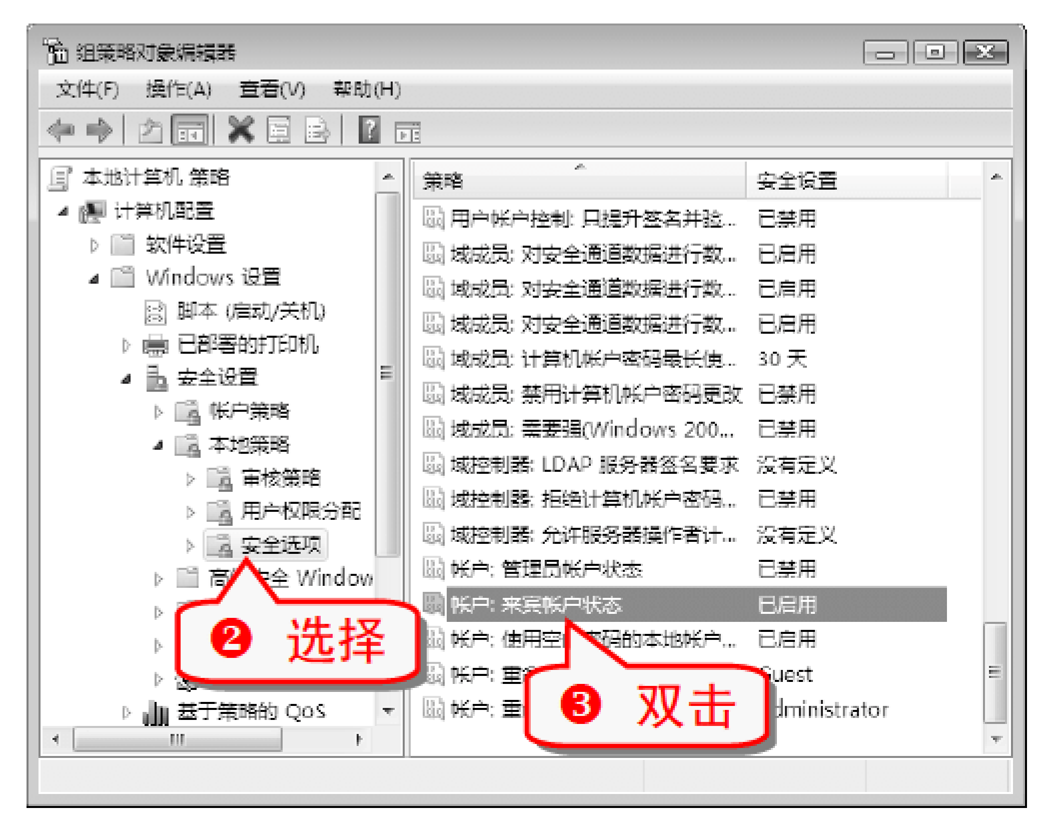


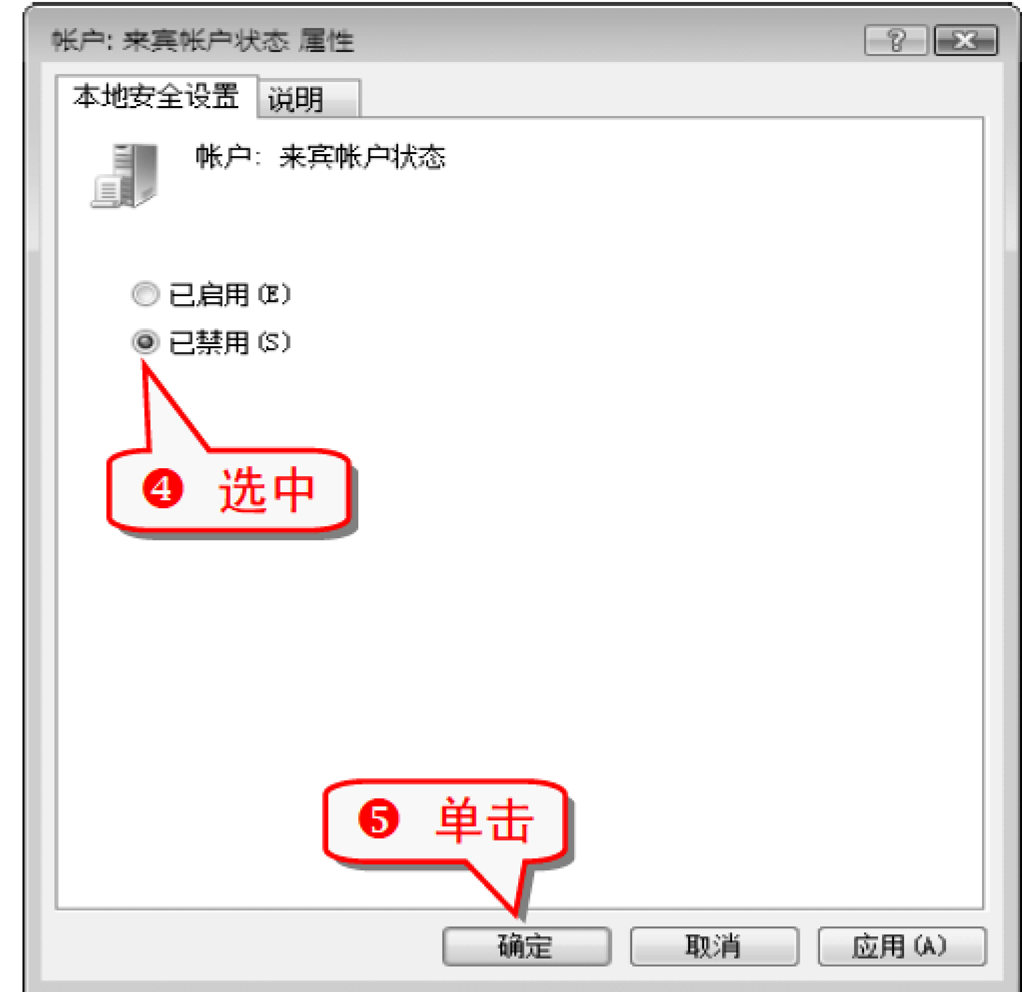
技巧136 彻底禁用来宾账户

黑客能通过提升来宾账户的权限，侵入电脑的系统，对系统的安全造成威胁，禁用来宾账户可以增加系统的安全性。

❶ 打开组策略对象编辑器。







技巧137　禁用 Windows Vista 自动播放功能

禁用 Windows Vista 的自动播放功能，可以让启动的多媒体设备或光盘不再弹出自动播放对话框，防止病毒通过多媒体设备自动运行。

❶ 选择“开始”→“控制面板”命令。

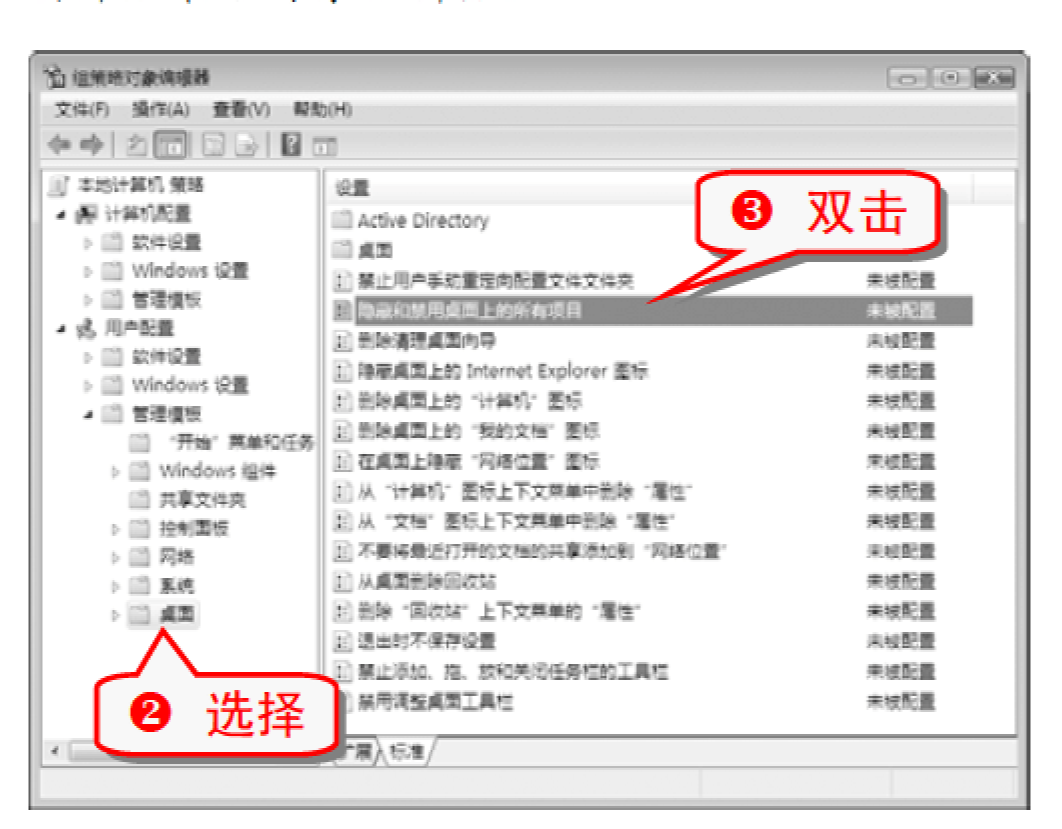


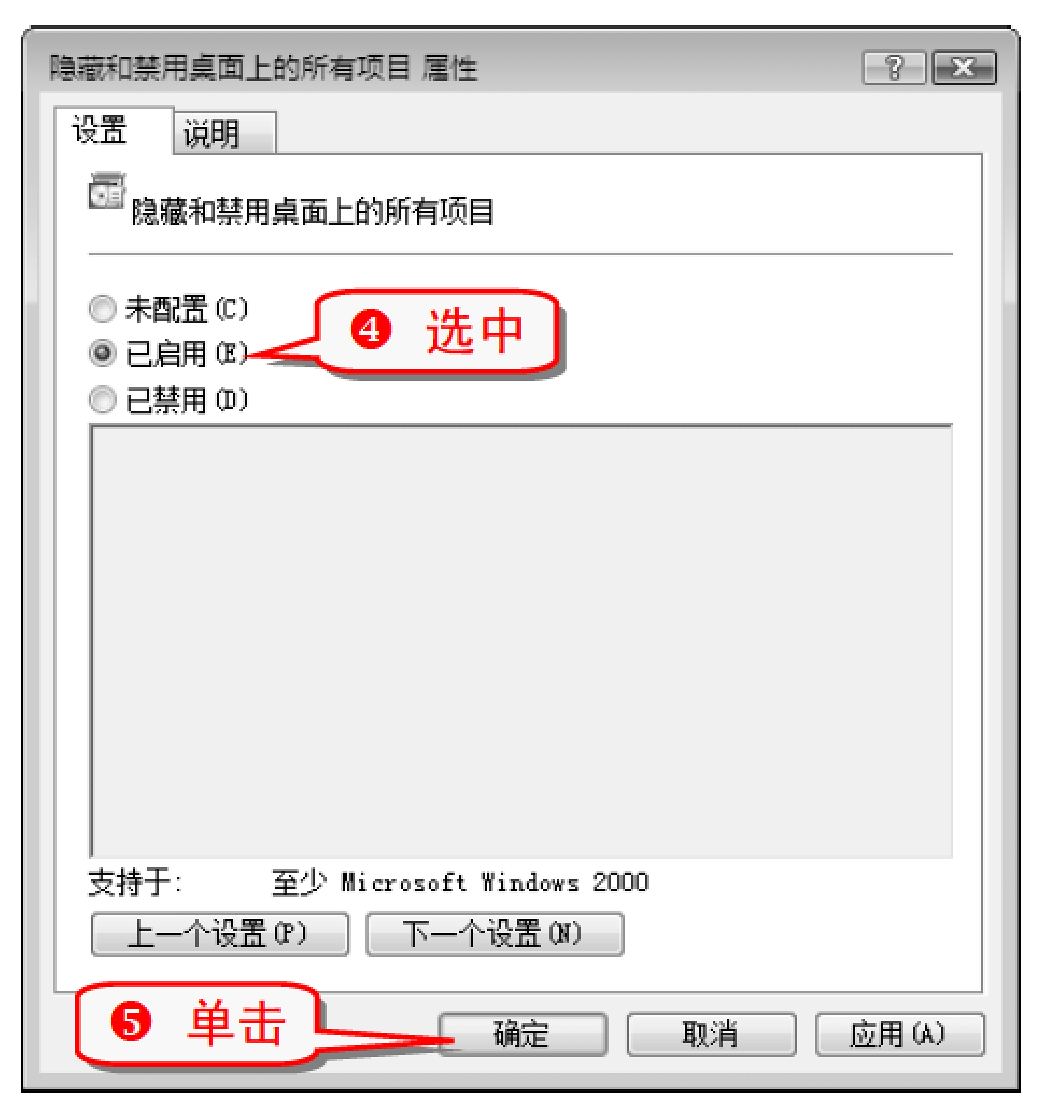


技巧138　禁止更改桌面的设置

通过设置组策略对象编辑器可以禁止用户更改桌面设置并将桌面上所有图标隐藏起来，增加系统的安全性。

❶ 打开组策略对象编辑器。



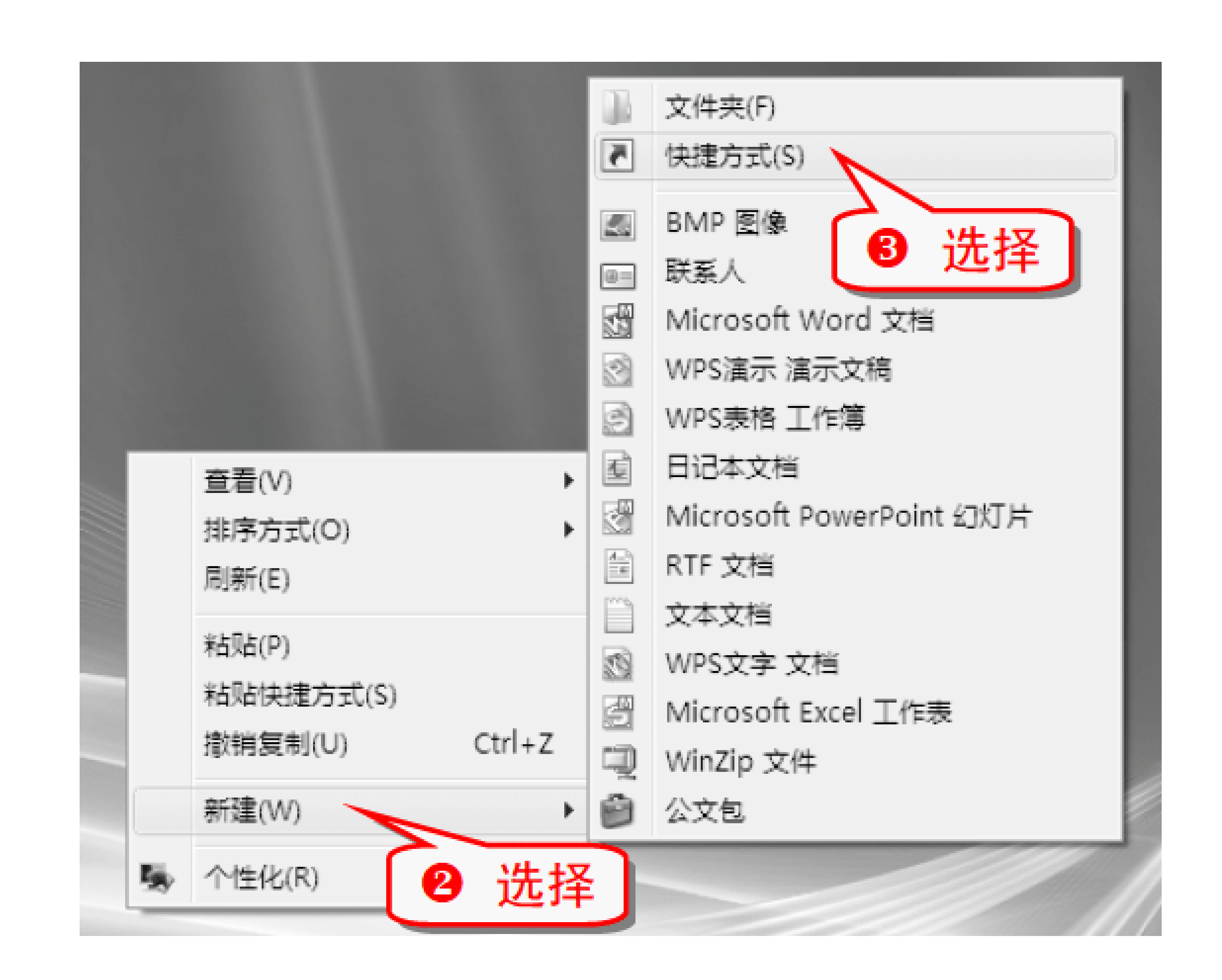


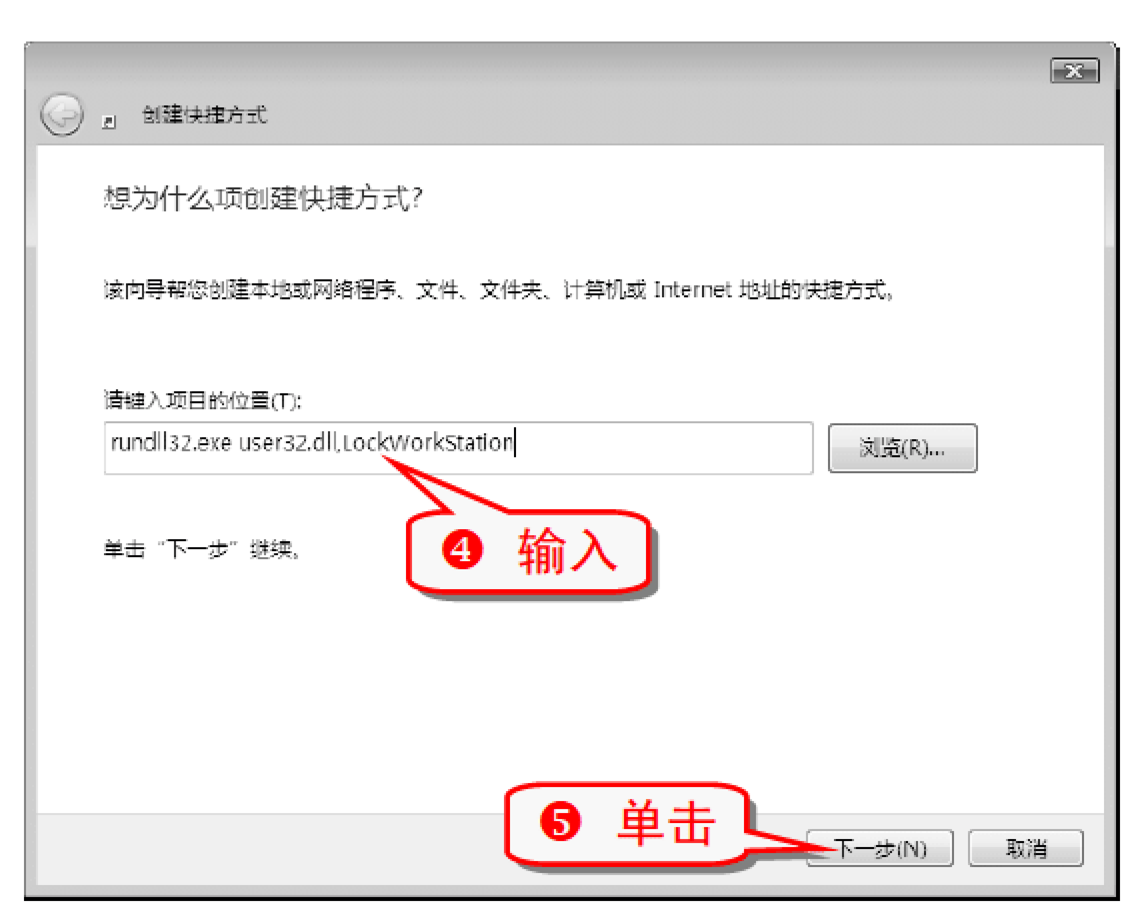


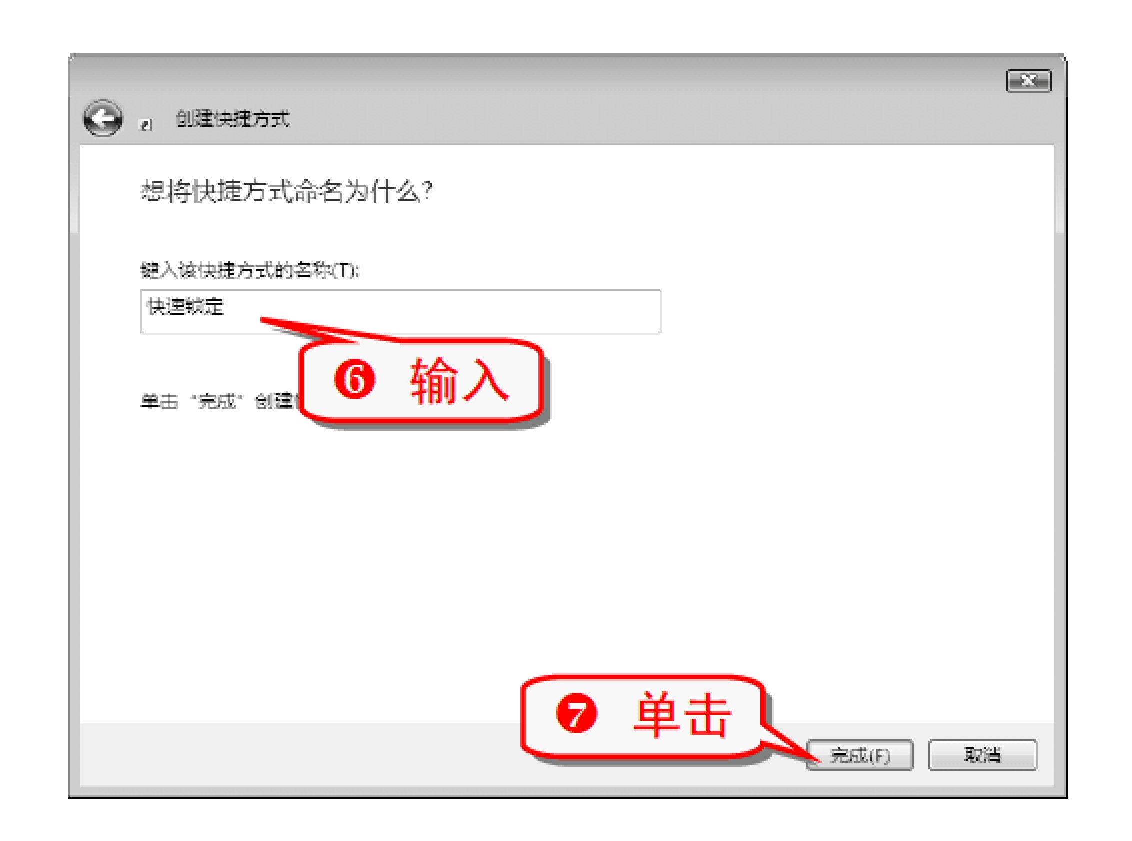
技巧139 建立快捷方式锁定桌面

在 Windows Vista 系统中，可以建立桌面快捷方式用来随时锁定电脑，而不用借助第三方软件。

❶ 右击桌面空白处，弹出快捷菜单。





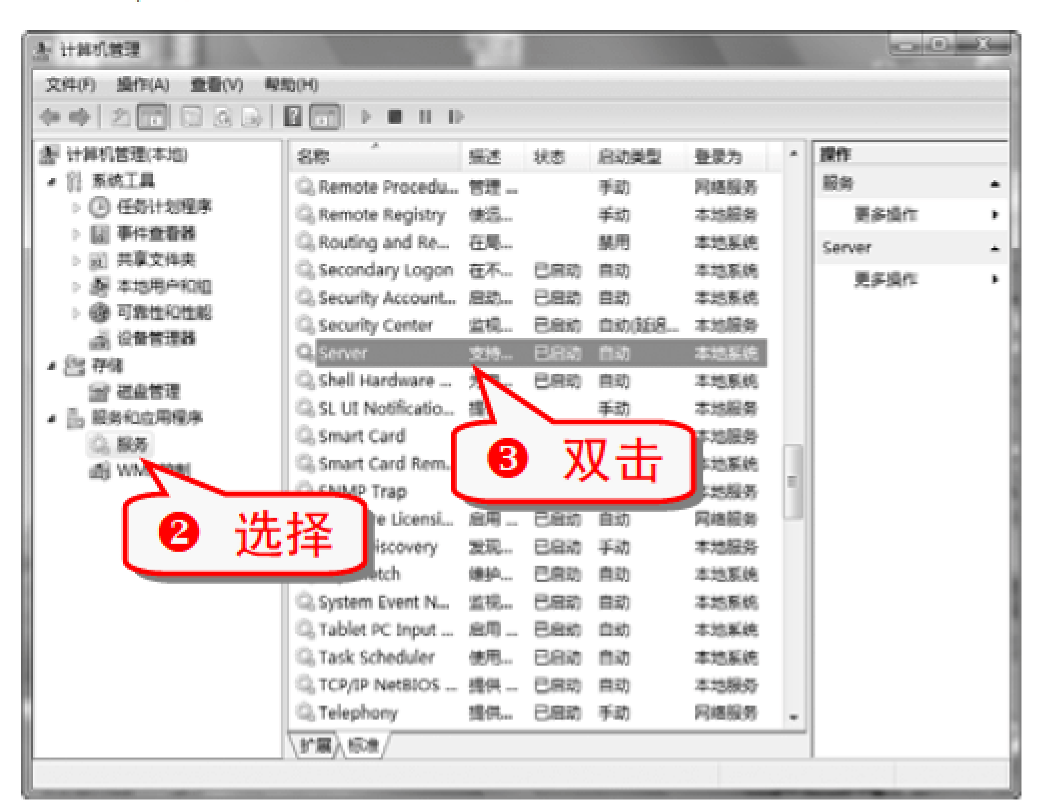


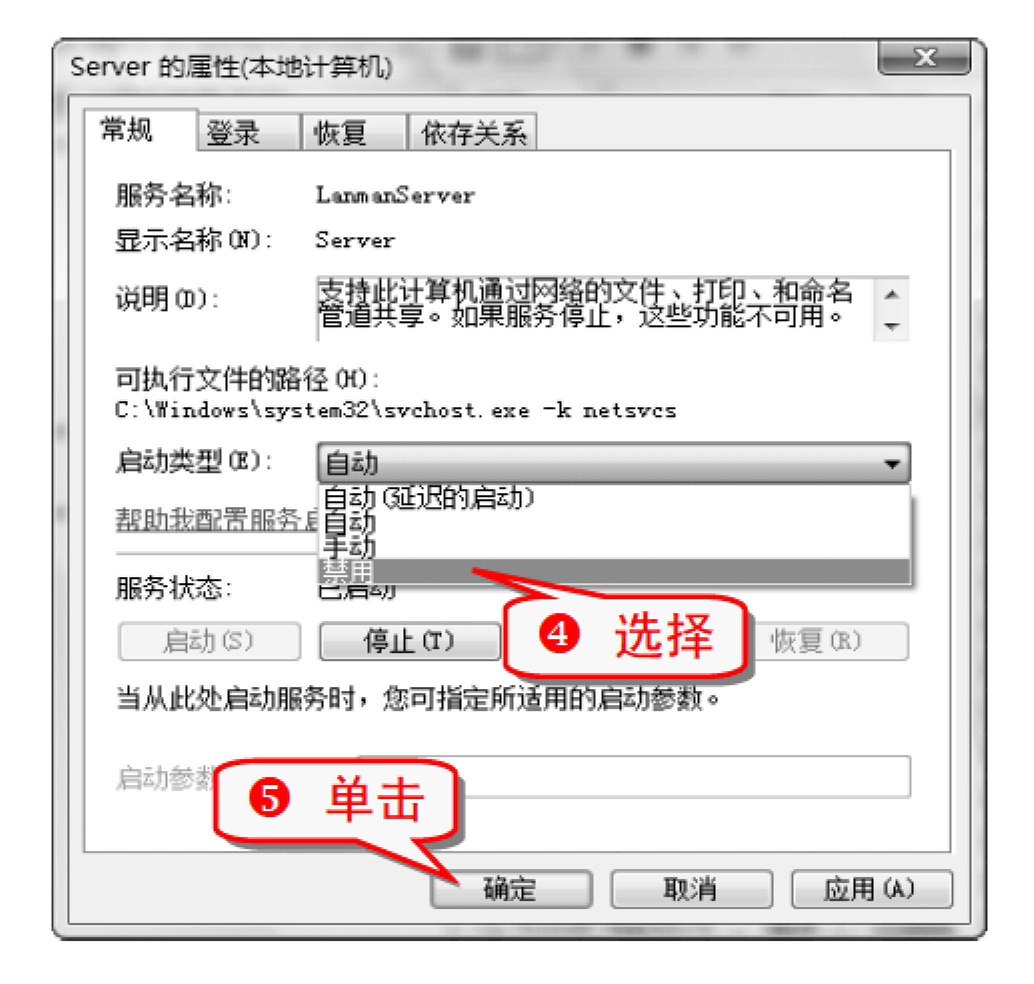
❽ 桌面上生成一个快捷方式，双击这个快捷方式就可以快速锁定电脑。

技巧140 禁用系统的默认共享设置

在 Windows Vista 系统中，在默认情况下硬盘和文件的共享设置是启用的，不利于系统的安全，因而有必要将其禁用。

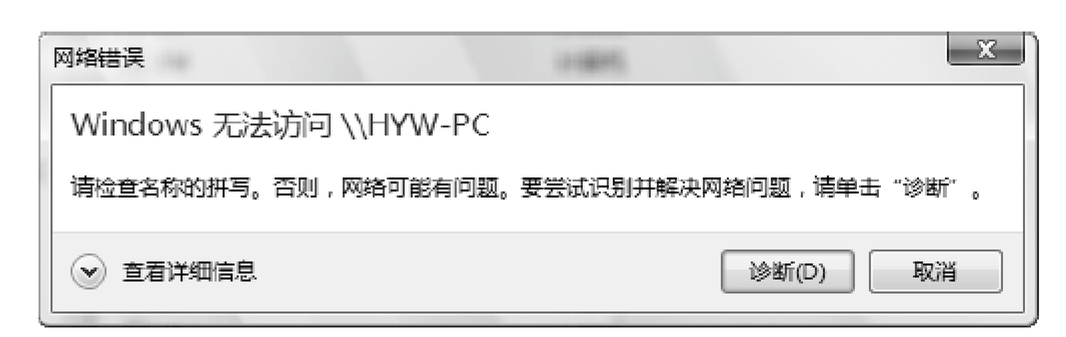
❶ 右击“计算机”图标，在弹出的快捷菜单中选择“管理”命令。







❻ 通过局域网访问这台电脑时弹出如下对话框。



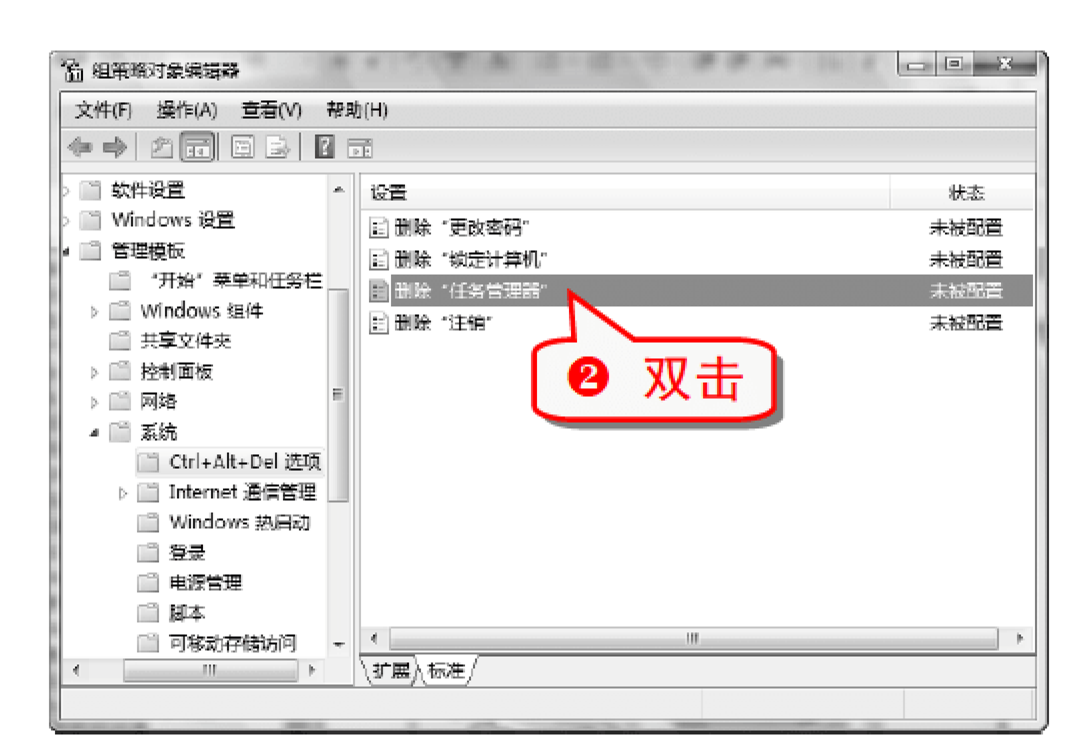

注　意　事　项

设置在注销或重新启动电脑后才能生效

技巧141　禁用任务管理器

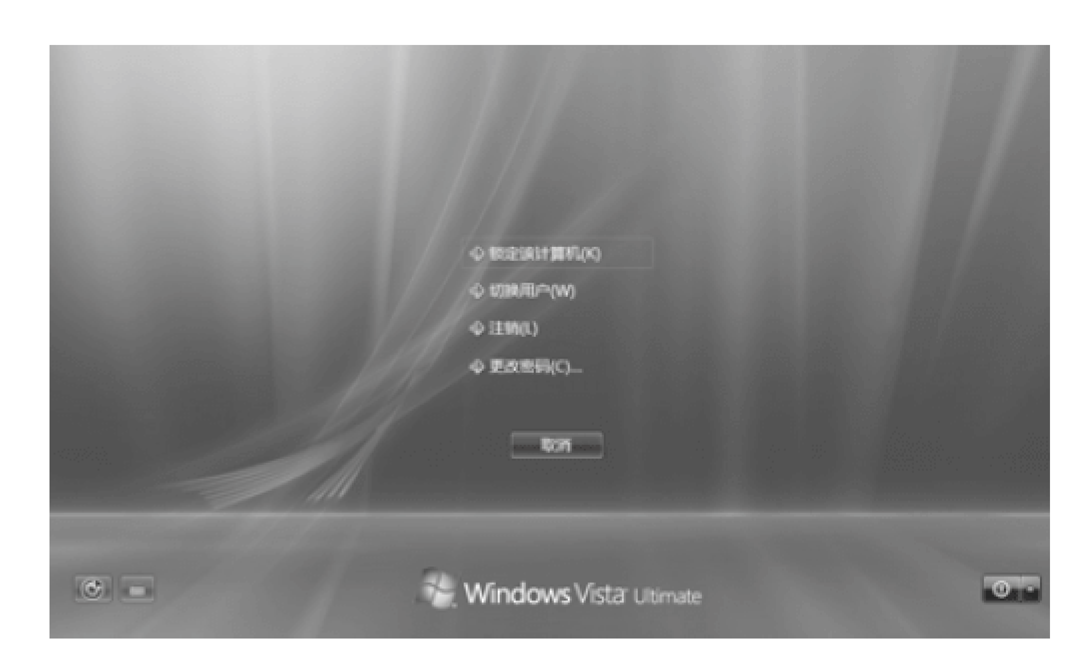
任务管理器可以查看当前电脑所有的应用程序、进程以及服务，因而将其禁用有利于系统的安全。

❶ 打开组策略对象编辑器，选择“用户配置”→“系统”→“Ctrl + Alt + Del 选项”选项。





❺ 按下 Ctrl + Alt + Del 组合键，可以发现不显示任务管理器。



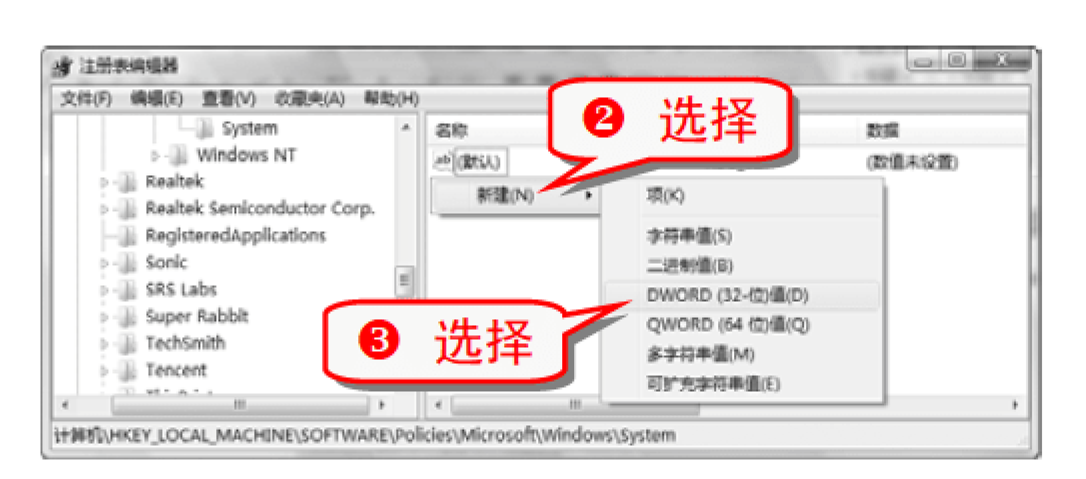
注　意　事　项

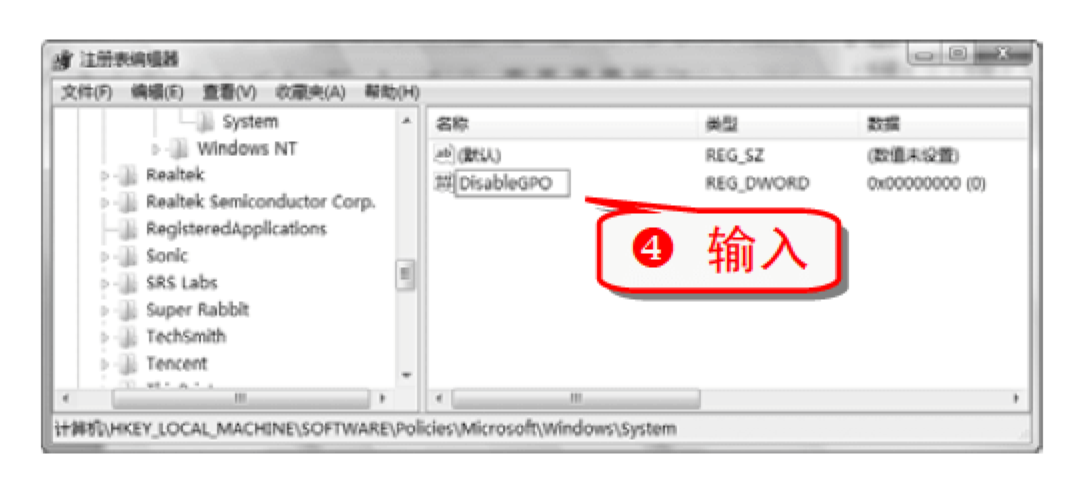
只要将删除“任务管理器”设置为已禁用未配置就可以重新启用任务管理器。

技巧142　禁止使用域的组策略

禁止使用域的组策略，可以提高系统的安全性。

❶ 打开“注册表编辑器”窗口，展开 HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System 分支，并在右边窗格空白处右击。





❺ 选择 DisableGPO 选项并双击。



技巧143 限制对系统日志文件的访问

限制用户对系统日志文件的访问，避免误操作或者恶意软件对日志文件进行篡改，可以维护系统的安全。

❶ 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog 分支。

❷ 依次选择 Application、Security 和 System，在右边窗格处选中相同的子键 RestrictGuestAccess 后双击。







技巧144 当某项服务启动失败时进行错误检测

当系统启动某项服务失败时进行错误检测，可以将错误原因发送至用户，提示用户完成操作。

❶ 打开注册表编辑器窗口，展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ErrorControl 分支。

❷ 选择 ErrorControl 选项并双击。



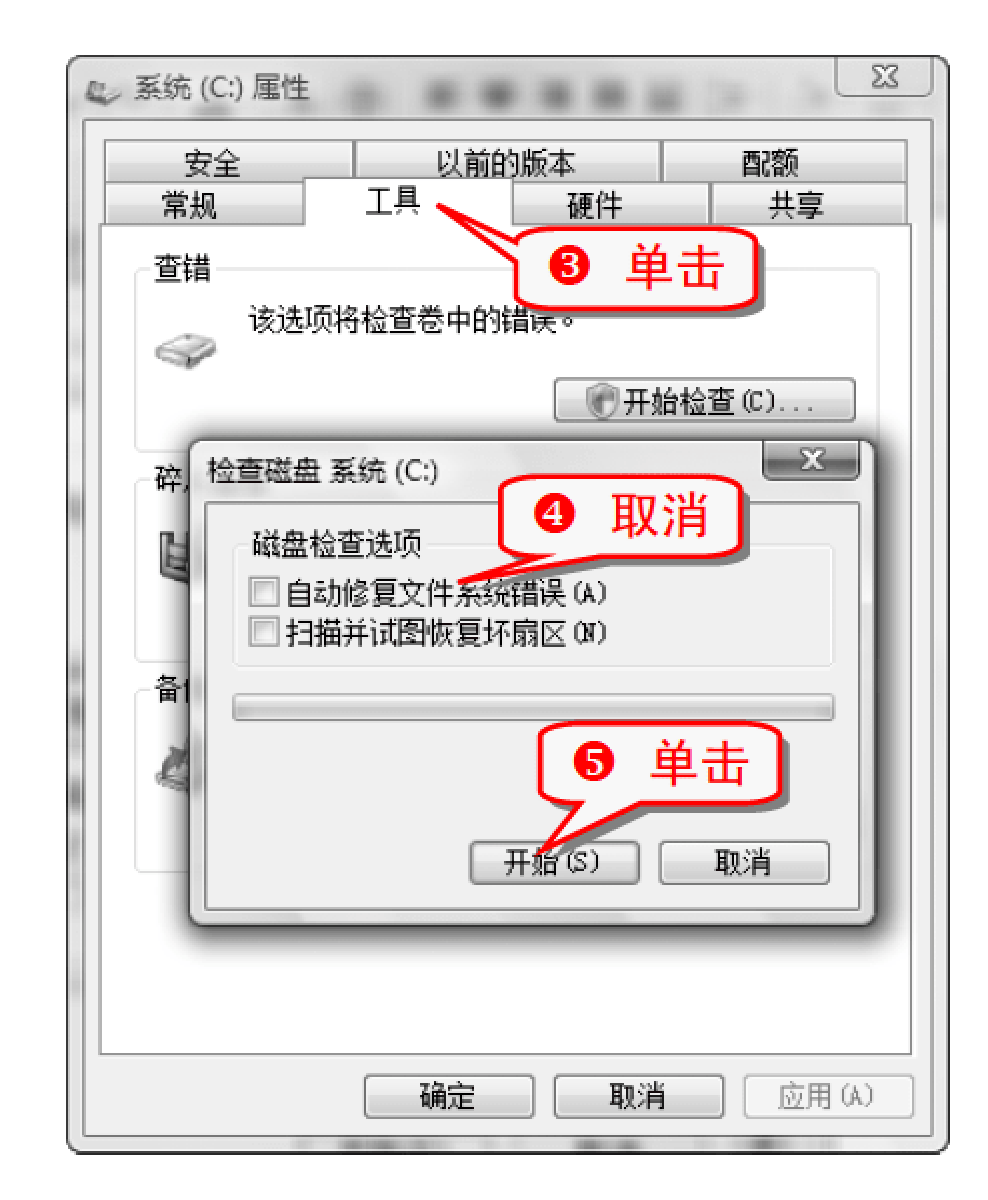
技巧145 对磁盘进行定期检查

电脑在使用过程中，由于长期对磁盘进行读写操作，可能会使磁盘的文件系统受到破坏并产生坏扇区，从而降低磁盘的使用效率。

Windows Vista 自带了一个磁盘扫描工具，可以方便地对磁盘分区进行扫描并修复一些简单的错误。

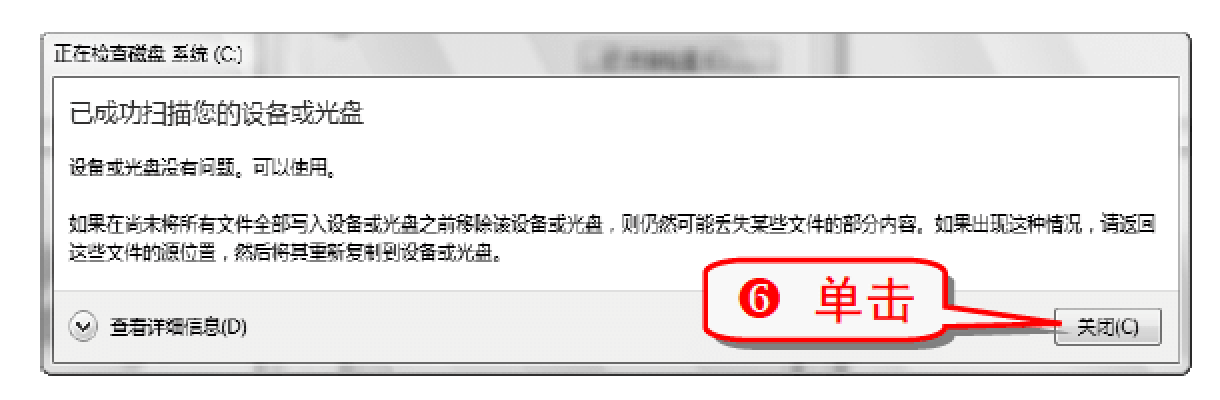
❶ 双击桌面上的“计算机”图标，弹出“计算机”窗口，右击需要进行检查的磁盘分区。











知 识 补 充

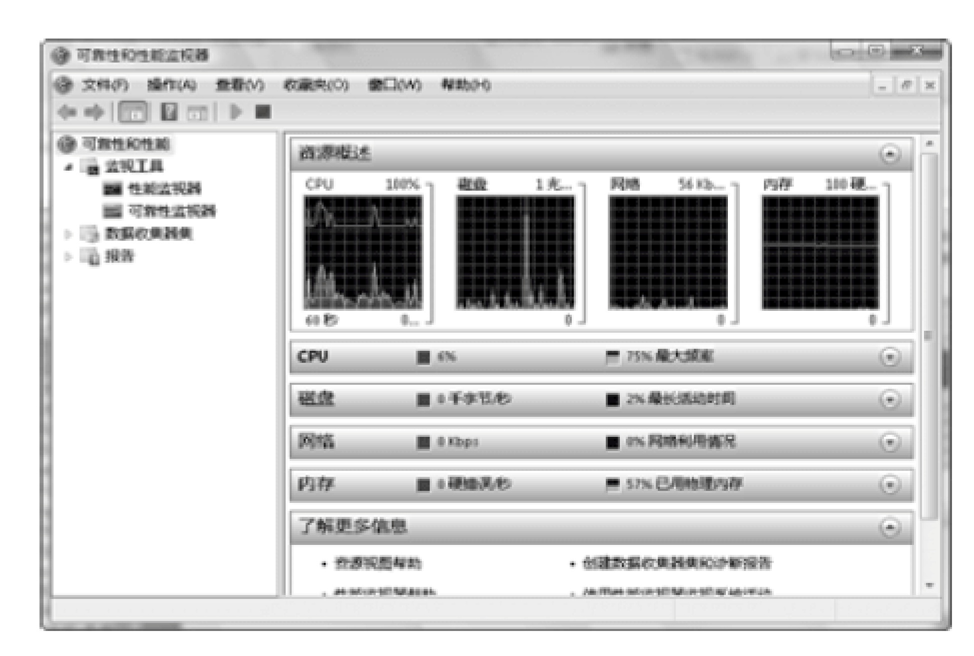
在检查磁盘系统对话框中，选中“自动修复文件系统错误”复选框后，由于检查程序需要单独访问系统分区上的一些文件，而这些文件又很可能正在被操作系统使用，所以单击“开始”按钮后，程序会提示“是否要在下次启动计算机时检查硬盘错误？”，如果想在下一次重新启动电脑时执行修复操作，单击 计划磁盘检查 按钮；如果不想在下次重新启动电脑时执行修复操作，单击“取消”按钮即可。

技巧146 对系统进行实时监控

任何操作系统的稳定运行都离不开操作者的精心维护。Windows Vista 的强大系统功能，更需要经常维护才能发挥其最大的功效。

❶ 双击桌面上的“计算机”图标，在弹出的“计算机”窗口左边的文件夹列表项，展开“控制面板”→“系统和维护”分支。

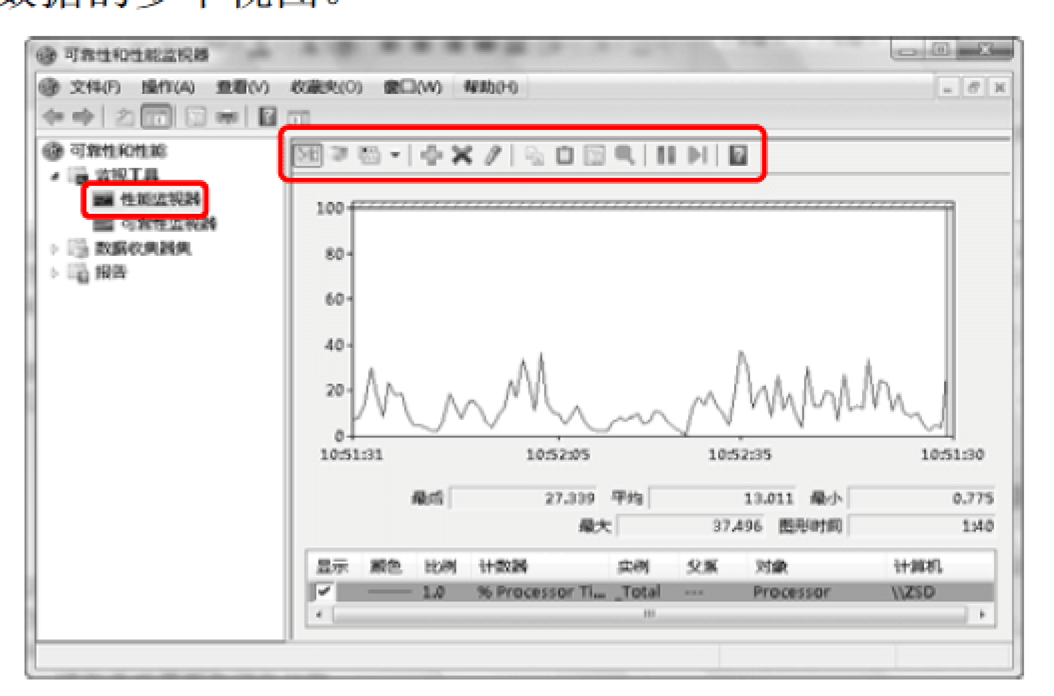




(1) 性能监视器

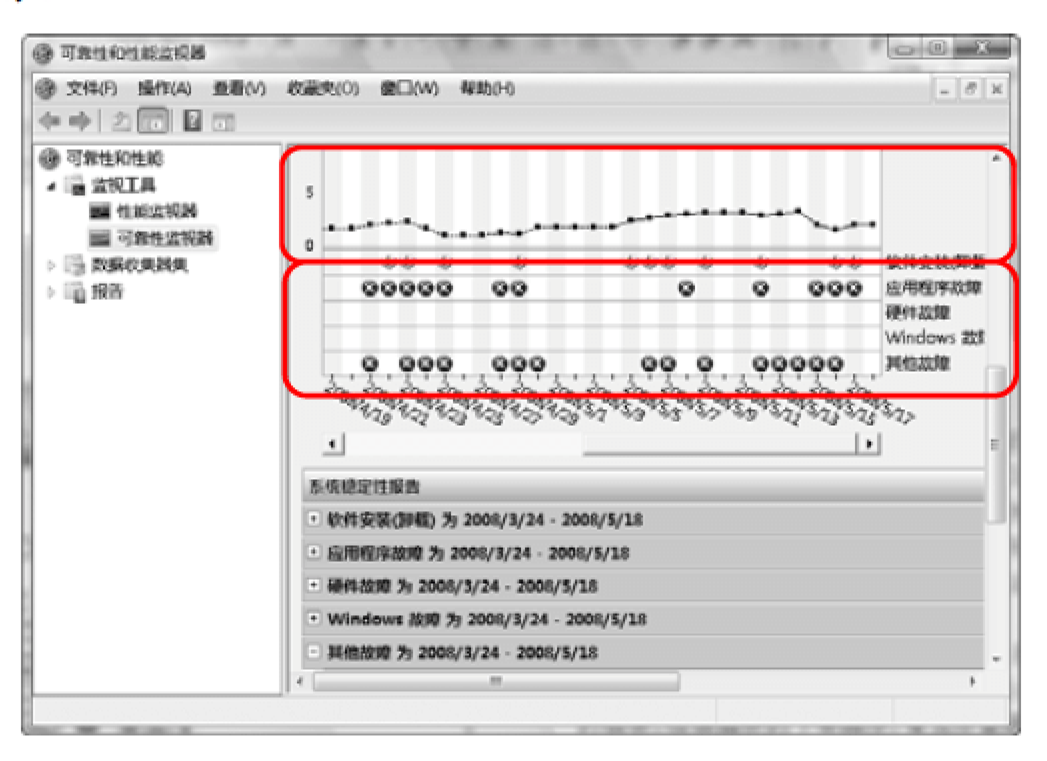
在打开的“可靠性和性能监视器”窗口中单击“性能监视器”选项，即可进入具体查看窗口。在该窗口中可以查看实时或历史的数据图表，以了解内置的 Windows 性能计数器。

用户还可以通过创建自定义数据收集器将性能计数器添加到性能监视器。其特征在于可以直观地查看性能日志数据的多个视图。



(2) 可靠性监视器

在打开的“可靠性和性能监视器”窗口中单击“可靠性监视器”选项，即可进入具体查看窗口。在该窗口中可以查看系统稳定性的大体情况以及趋势分析，同时还显示出可能会影响系统总体稳定性的个别事件的详细信息，例如软件安装、应用程序故障、硬件故障以及 Windows 故障等。



专 家 坐 堂

可靠性监视器最多可以保留一年的系统稳定性和可靠性事件的历史记录。在图表中上半部分显示了稳定性指数，下半部分可以跟踪可靠性事件，有助于测量系统的稳定性，或者提供有关软件安装和删除的相关信息。

技巧147 设置家长控制功能

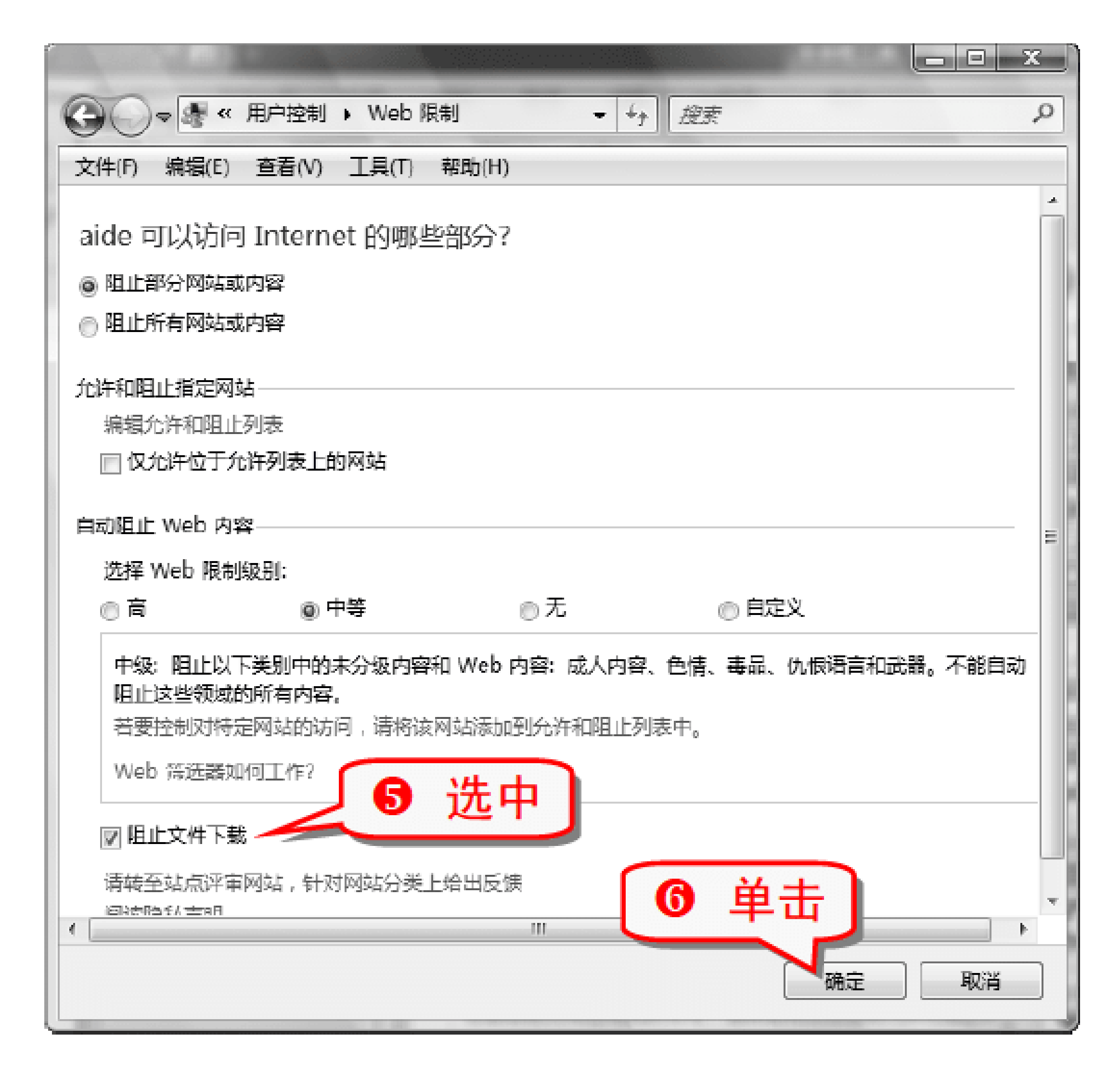
家长控制功能是 Windows Vista 系统提供给家长们的一项省心的家庭电脑使用控制功能，可以通过家长控制功能对儿童使用电脑的方式进行协助管理。例如，您可以限制儿童对网站的访问权限、登录的时间长短、可以玩的游戏以及可以运行的程序等。

❶ 在打开的“控制面板”窗口中单击“用户帐户和家庭安全”区域下的“为所有用户设置家长控制”链接，打开“家长控制”窗口。





❹ 在“Windows 设置”选项组中单击“Windows Vista Web 筛选器”链接，弹出“Web 限制”对话框。





知 识 补 充

选中“阻止所有网站或内容”单选按钮将会导致使用该账户的用户不能浏览网页，选中“阻止文件下载”复选框会导致使用该账户的用户不能下载文件。

❼ 在“Windows 设置”选项组中单击“时间限制”链接，弹出“时间限制”对话框。



知 识 补 充

除了可以单击选择每个方格外，还可以使用拖动的方法来选择多个方格。

❾ 在“Windows 设置”栏中单击“游戏”链接，在弹出“游戏控制”对话框中选中 ◉ 否 单选按钮，取消该用户玩任何游戏的权限，设置完成后单击“确定”按钮。

❿ 在“Windows 设置”选项组中单击“允许和阻止特定程序”链接，在打开的对话框中选中“aide 只能使用我允许的程序”单选按钮，单击“确定”按钮完成设置。



注 意 事 项

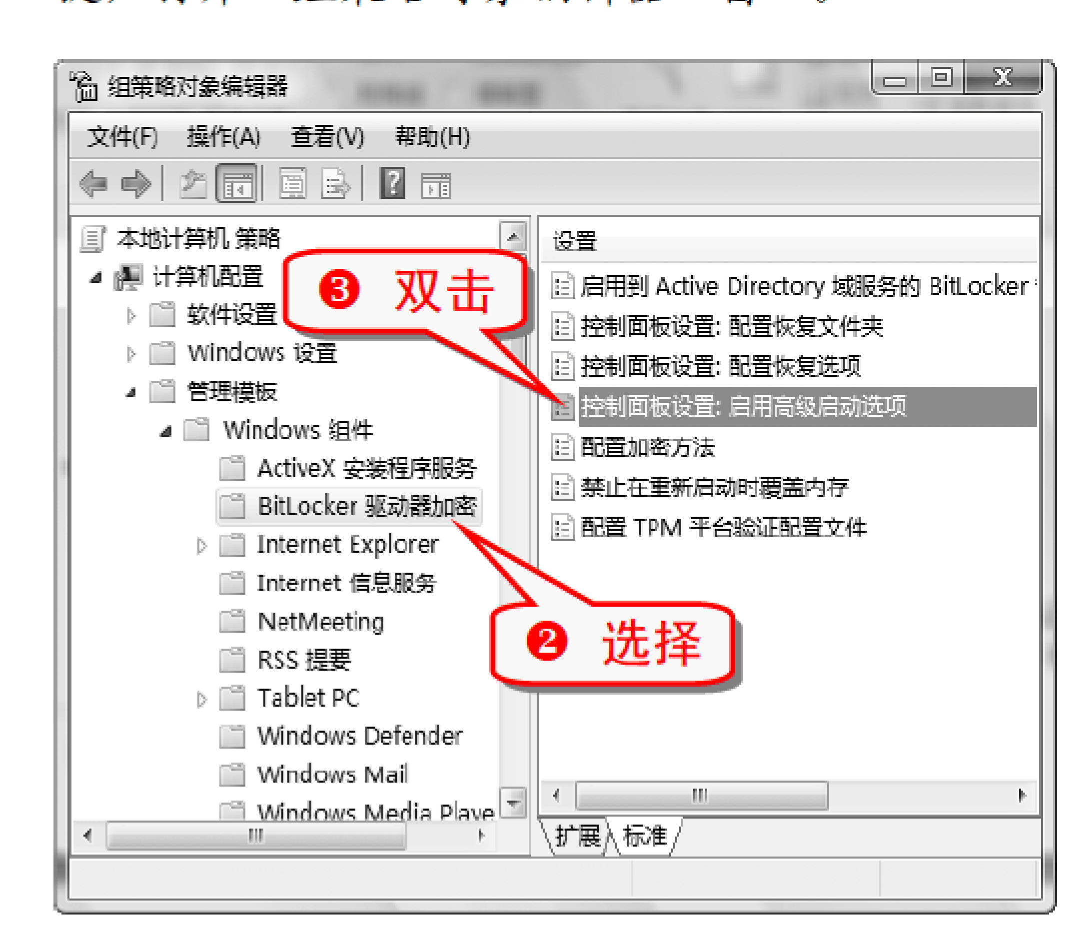
“家长控制”只能应用于标准用户账户，如果没有，可通过单击“创建新用户帐户”链接的方式来创建一个标准的用户账户。

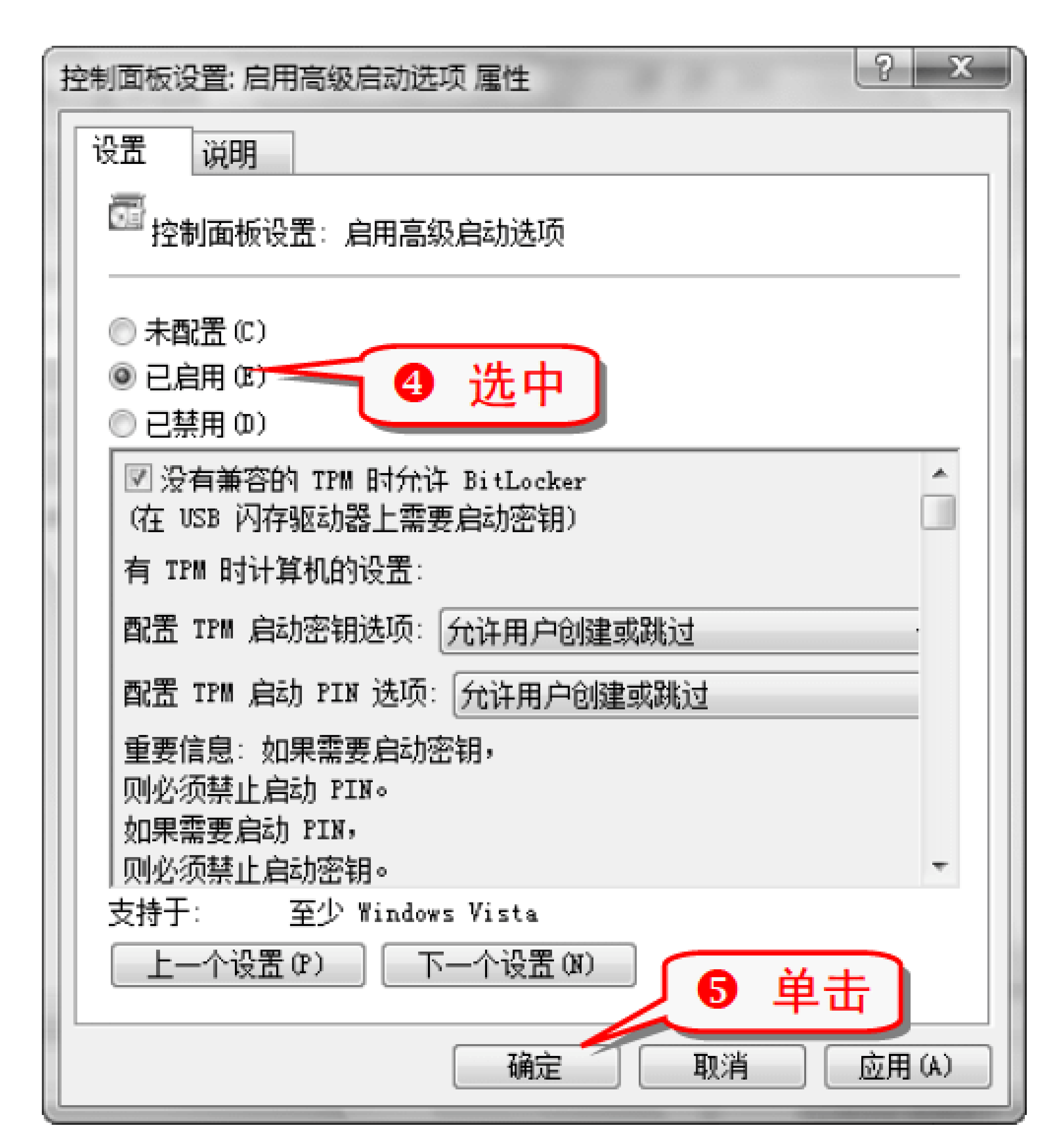
技巧148　使用 BitLocker 保护系统数据安全

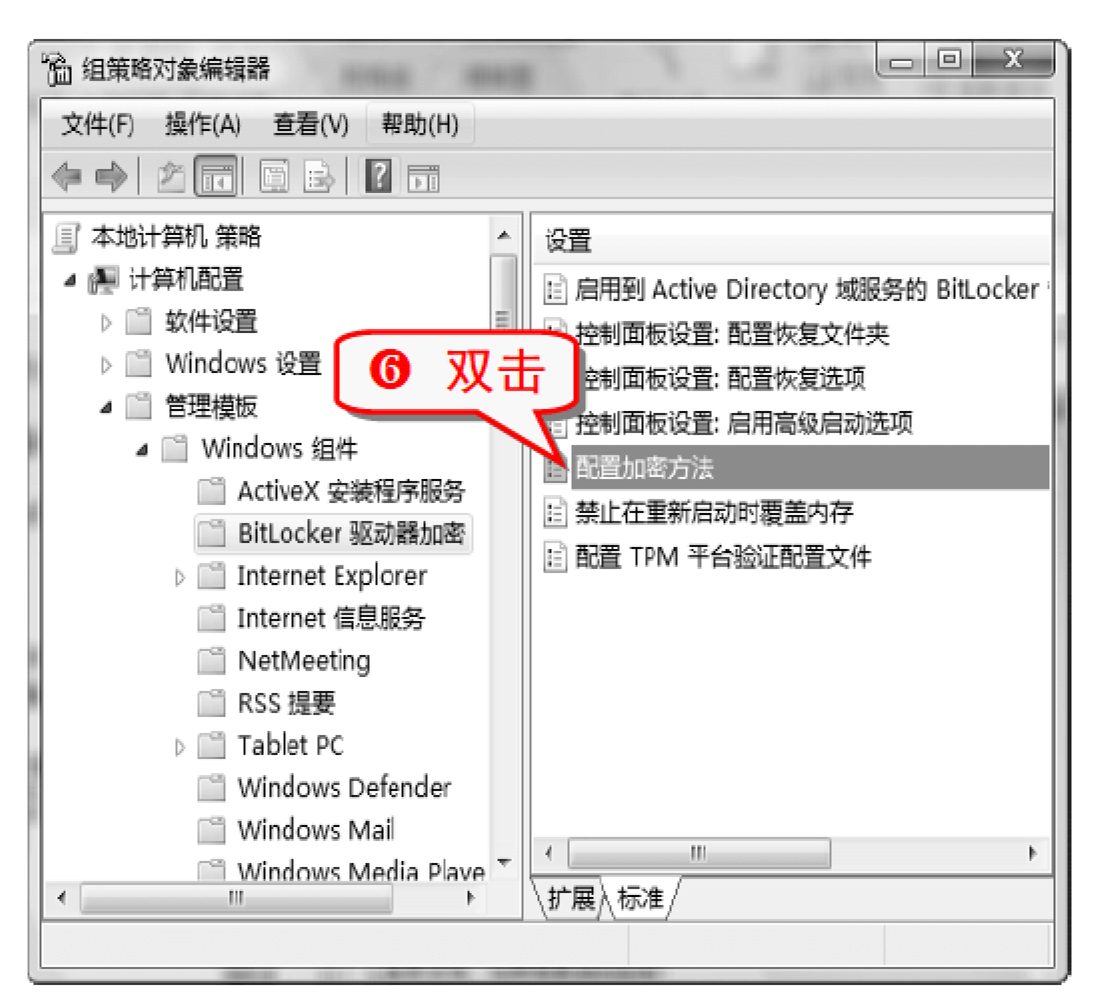
在 Windows Vista 系统中，新增加了一项 BitLocker 驱动器加密功能，可以最大程度地保障系统数据安全。BitLocker 以“离线”方式提供了整卷的加密。

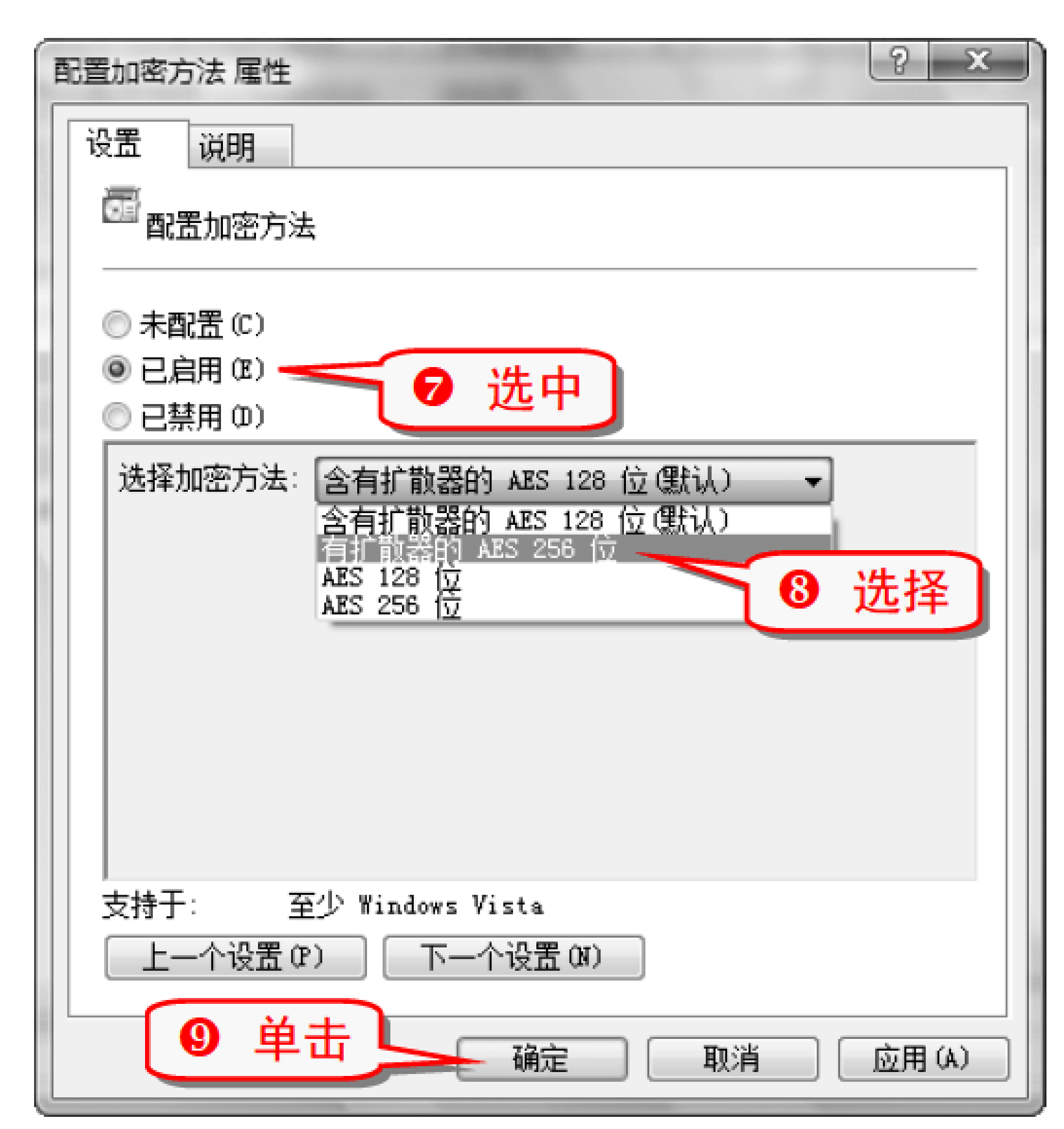
(1) 配置 BitLocker 环境

❶ 打开“运行”对话框，输入 gpedit.msc 命令，按下 Enter 键，打开“组策略对象编辑器”窗口。





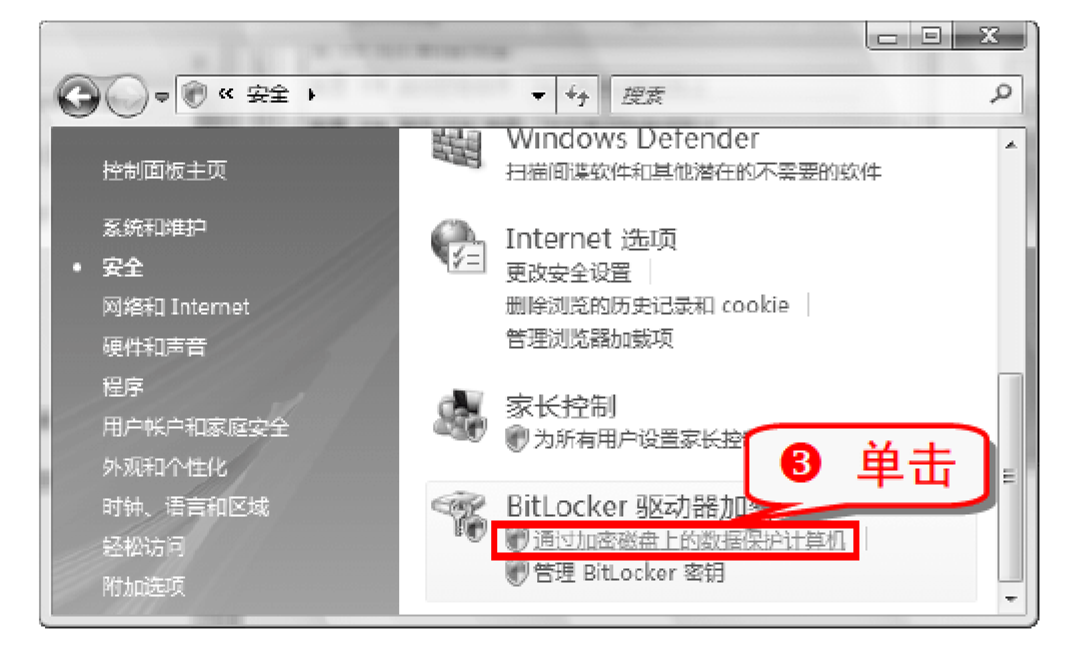




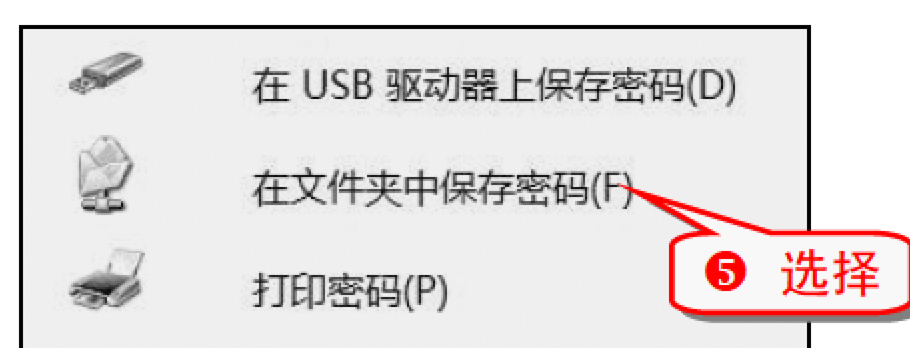
(2) 使用 BitLocker 工具

❶ 选择“开始”→“控制面板”命令。









❻ 插入 U 盘，单击“保存”按钮。

技巧149 Vista 优化大师使用全攻略

Vista 优化大师，号称 Windows Vista 系统优化软件中的瑞士军刀，其功能强大，给维护系统安全带来很大的方便。

(1) 内存及缓存优化

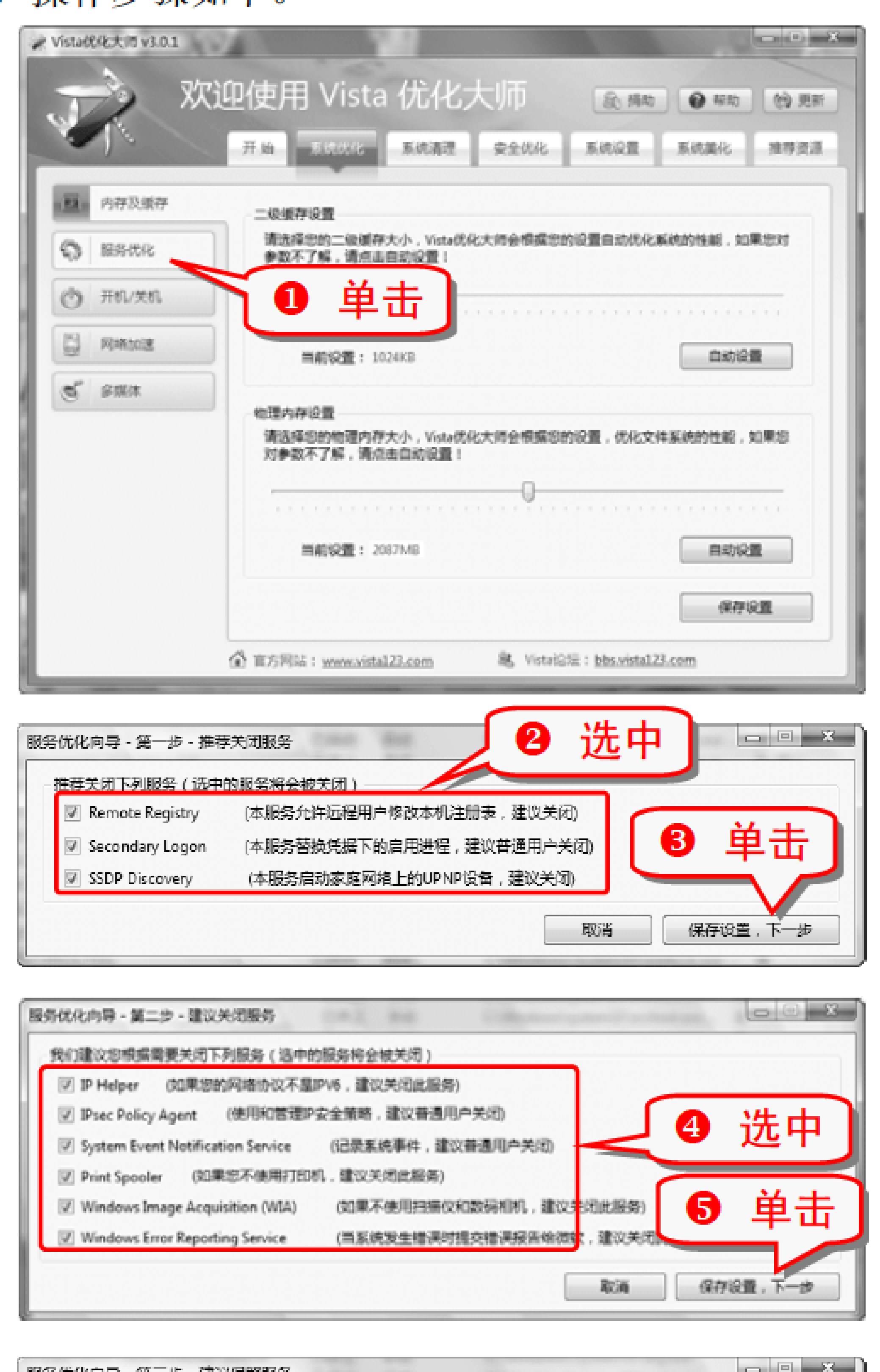
❶ 运行 Vista 优化大师。

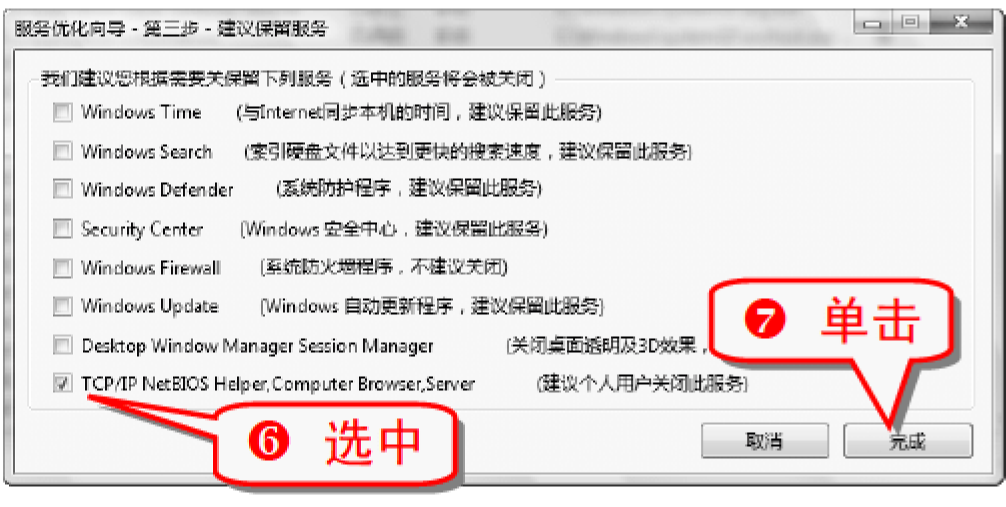


❹ 对于物理内存的优化设置也可以采用自动设置，如果对于这些功能比较了解，可以通过手动设置进行配置。

(2) 服务优化

对物理内存的优化设置完成后，需要对服务进行优化，操作步骤如下。







(3) 开机/关机优化

❶ 选择“开机/关机”选项，在右边的窗格中有选择地禁用一些功能。



(4) 多媒体优化

❶ 选择多媒体选项，在右边的窗格中有选择地禁用一些功能。



(5) 垃圾文件清理

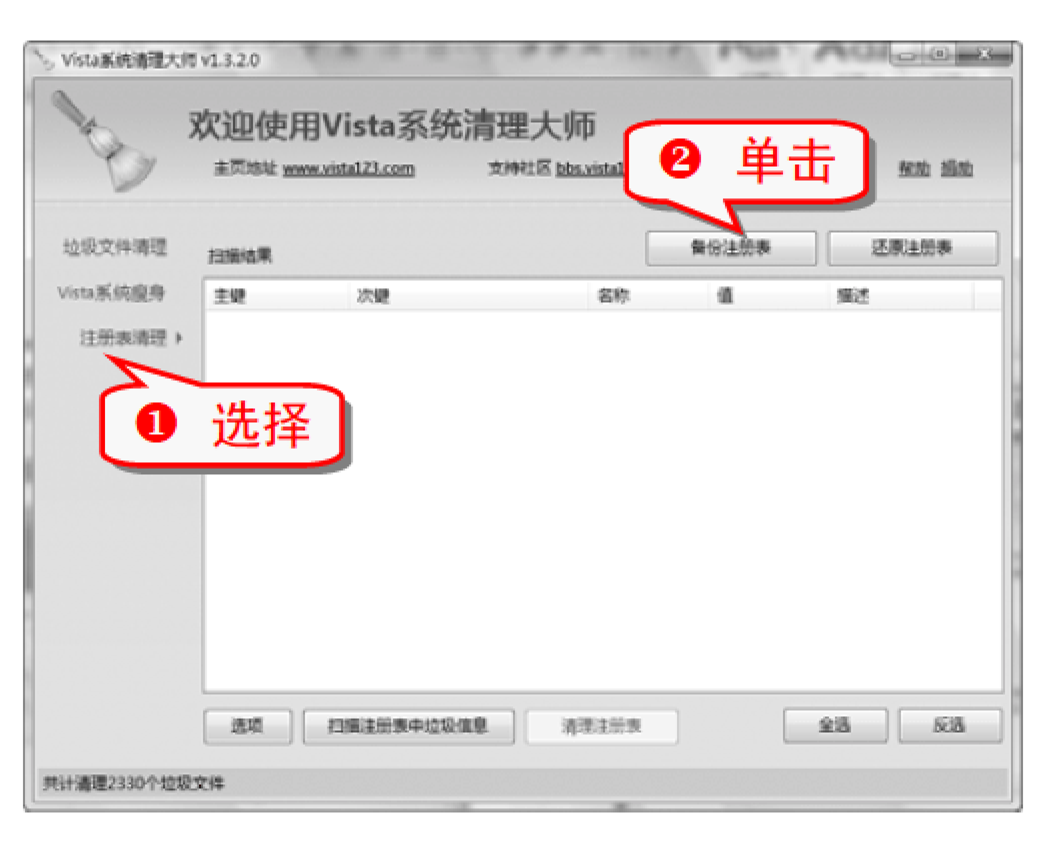
❶ 选择系统清理选项。

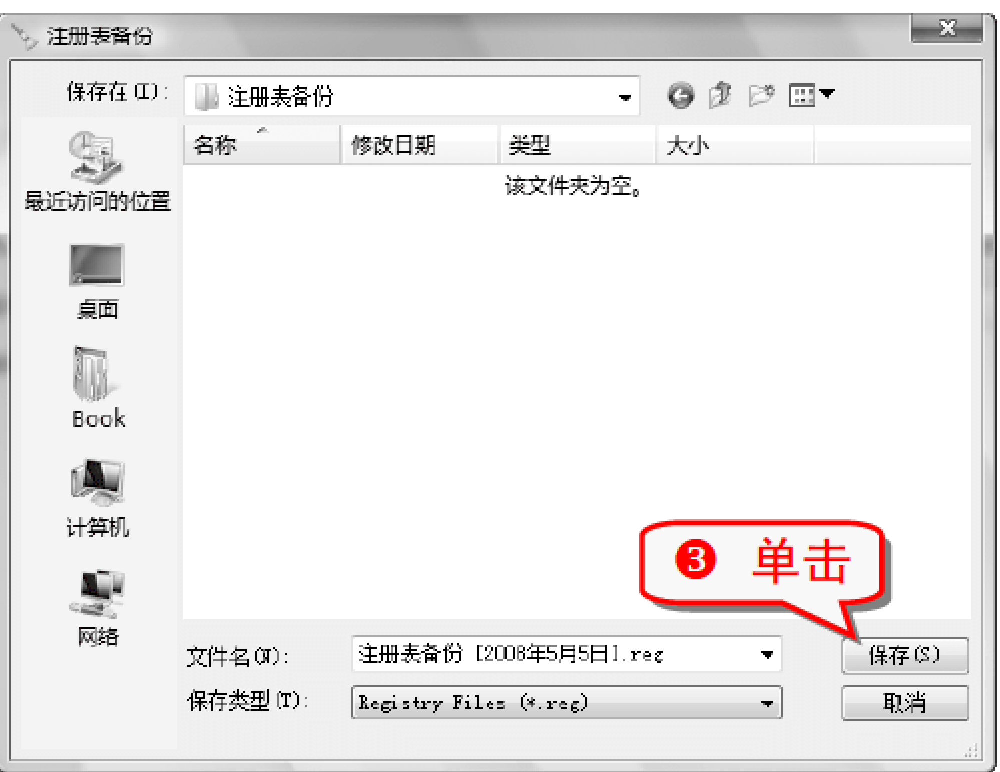




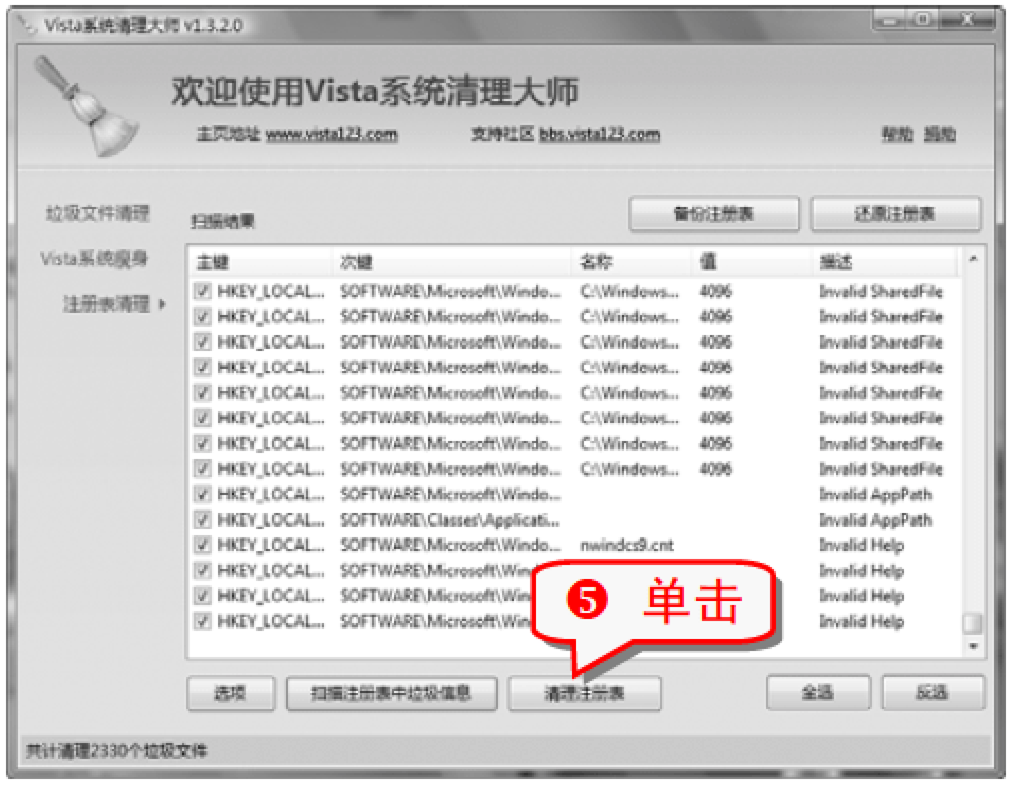
(6) 注册表清理

在清理注册表之前先进行备份，当注册表清理出现问题时，可以对其进行恢复。



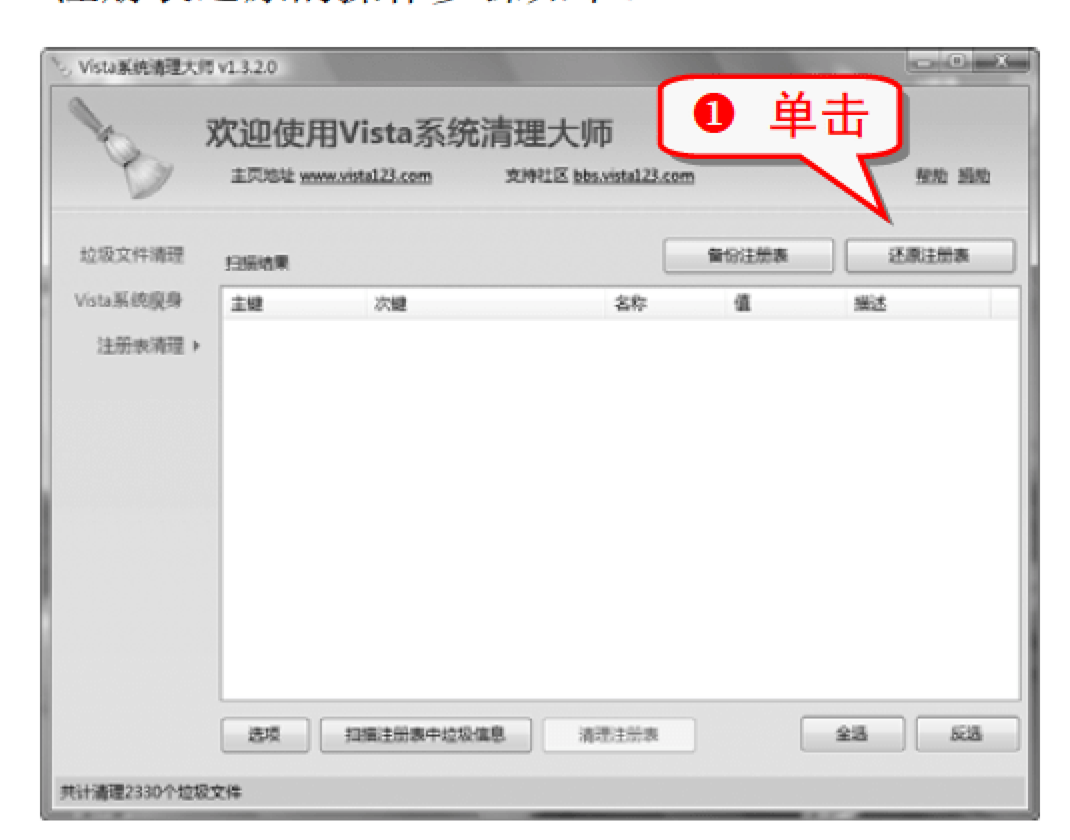






(7) 注册表还原

注册表还原的操作步骤如下。





(8) 系统安全设置

按照不同的需求有选择地选中下述的禁用选项。



技巧150 卸载流氓软件

“完美卸载”是一款功能强大的系统维护软件，可用于卸载掉系统中的“流氓”软件。

❶ 运行完美卸载软件。









专题六　电脑上网安全防护

内容导航

自从互联网诞生，网络安全问题就一直存在着，来自网络的威胁无处不在。掌握一定的上网安全防护技巧，可以有效地保护上网的安全，防止恶意网页危害系统。



- 拦截 Active 插件
- 屏蔽 IE 弹出窗口
- 禁止修改 IE 主页
- 设置 Cookie 访问权限
- 禁止 IE 的下载功能
- 屏蔽恶意网站技巧

技巧151　在傲游上轻松拦截 Active 插件

用户浏览网页时会出现提醒安装插件之类的消息，要避免出现这种情况，只要在傲游浏览器中进行简单的设置就可以了。

❶ 打开傲游浏览器。

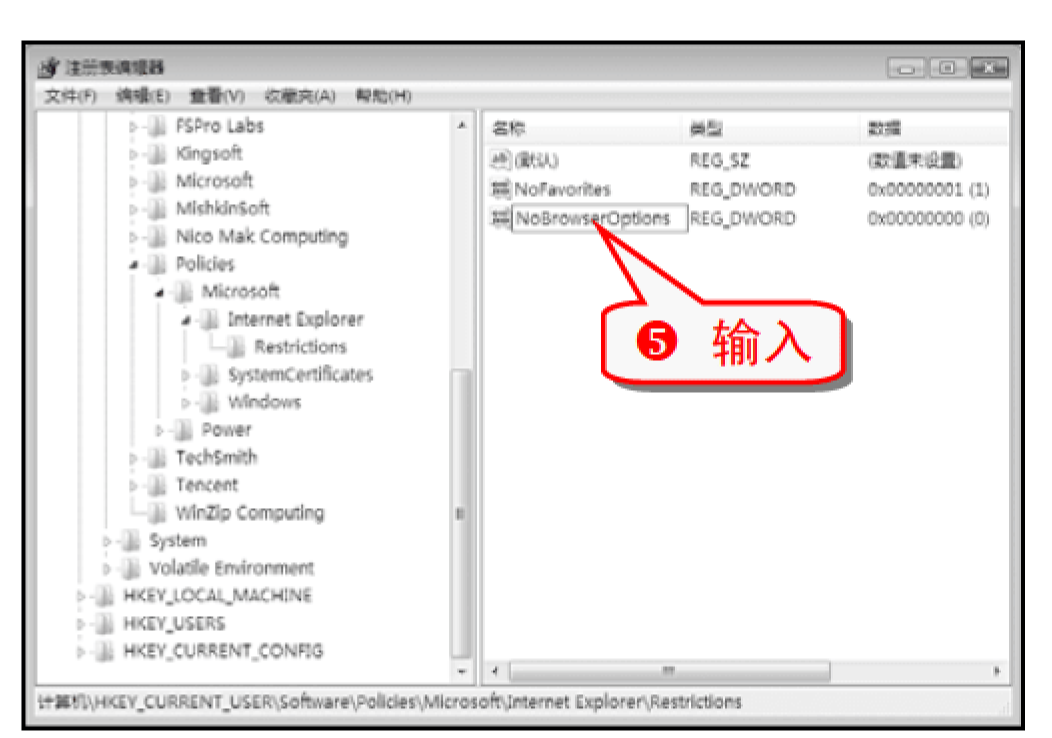


技巧152　禁止 IE 中的 Internet 选项

通过 Internet 选项可以对 IE 进行很多的设置，通过注册表禁止在“工具”中显示“Internet 选项”命令，可以保护 IE 的安全。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\InternetExplorer\Restrictions 分支。







技巧153　巧妙管理 IE 加载项

加载项可以为 IE 添加多种功能，但也有可能使网页不能正常显示或强制关闭网页，所以要巧妙管理 IE 加载项是很重要的。

❶ 打开 IE 浏览器，选择“工具”→“管理加载项”→“启用或禁用加载项”命令，弹出“管理加载项”对话框。

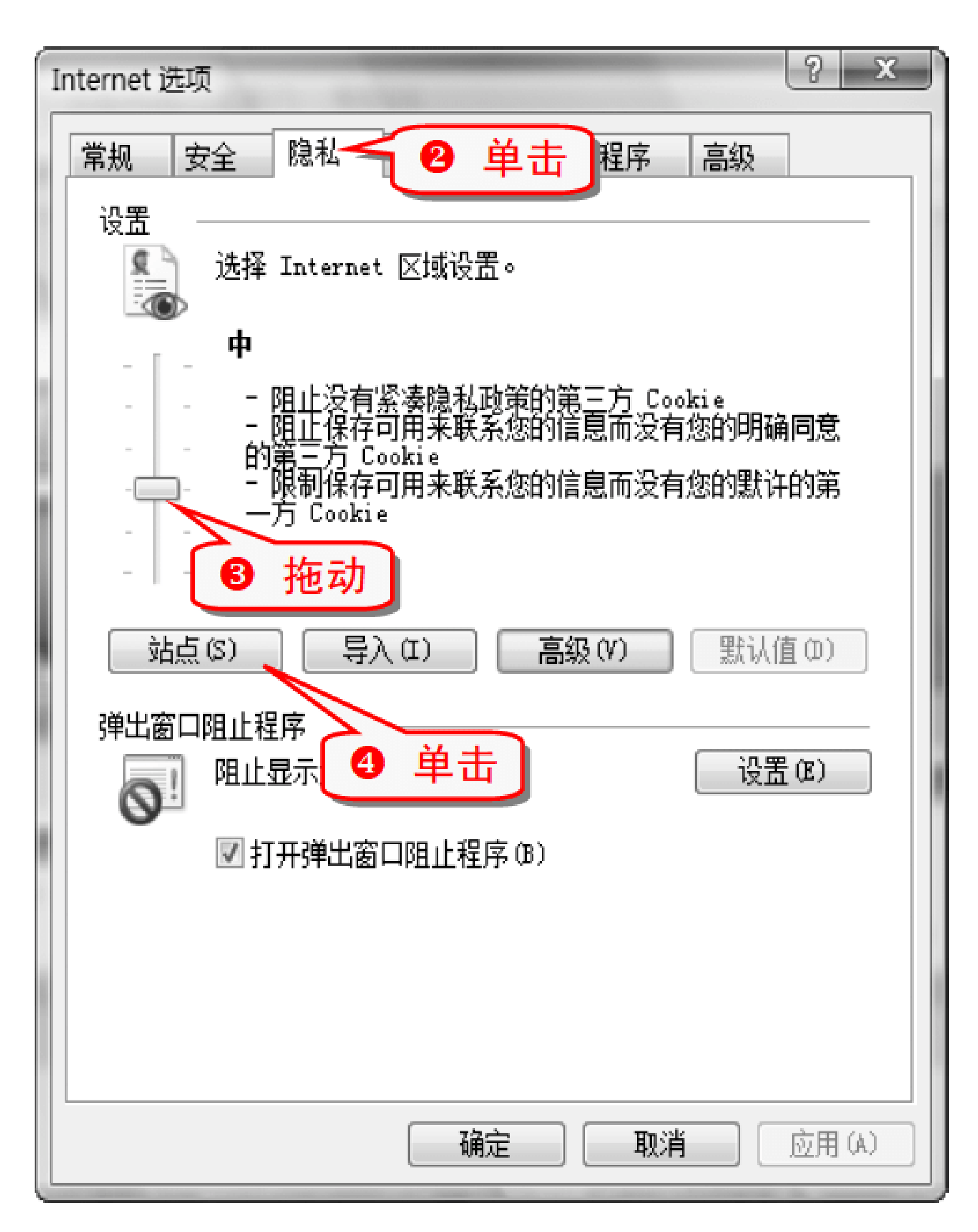


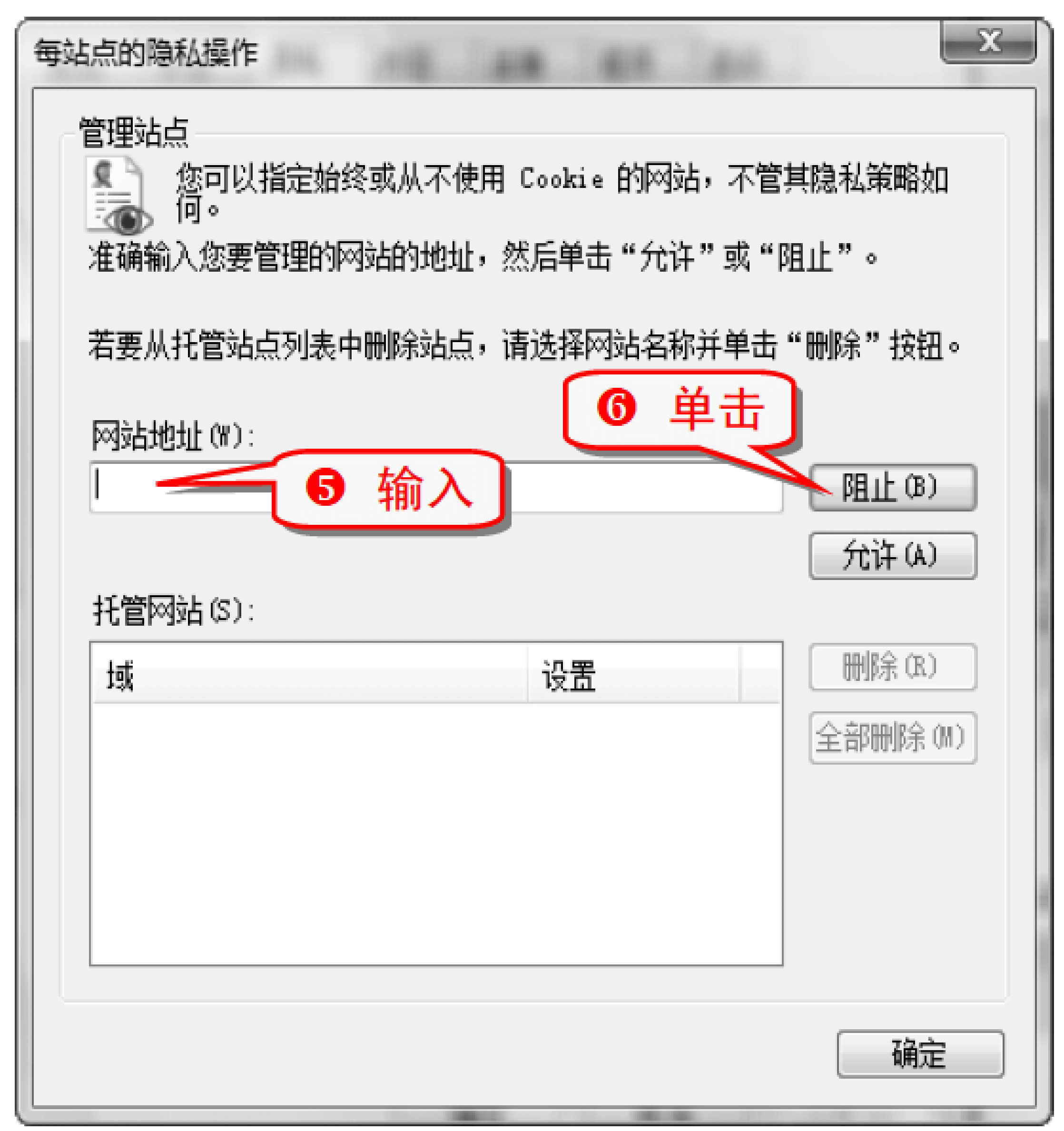
❷ 在“管理加载项”对话框中禁用非法的加载项。

技巧154　为 IE 设置 Cookie 的访问权限

管理好 Cookie，可以保障 IE 的安全性。

❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令。



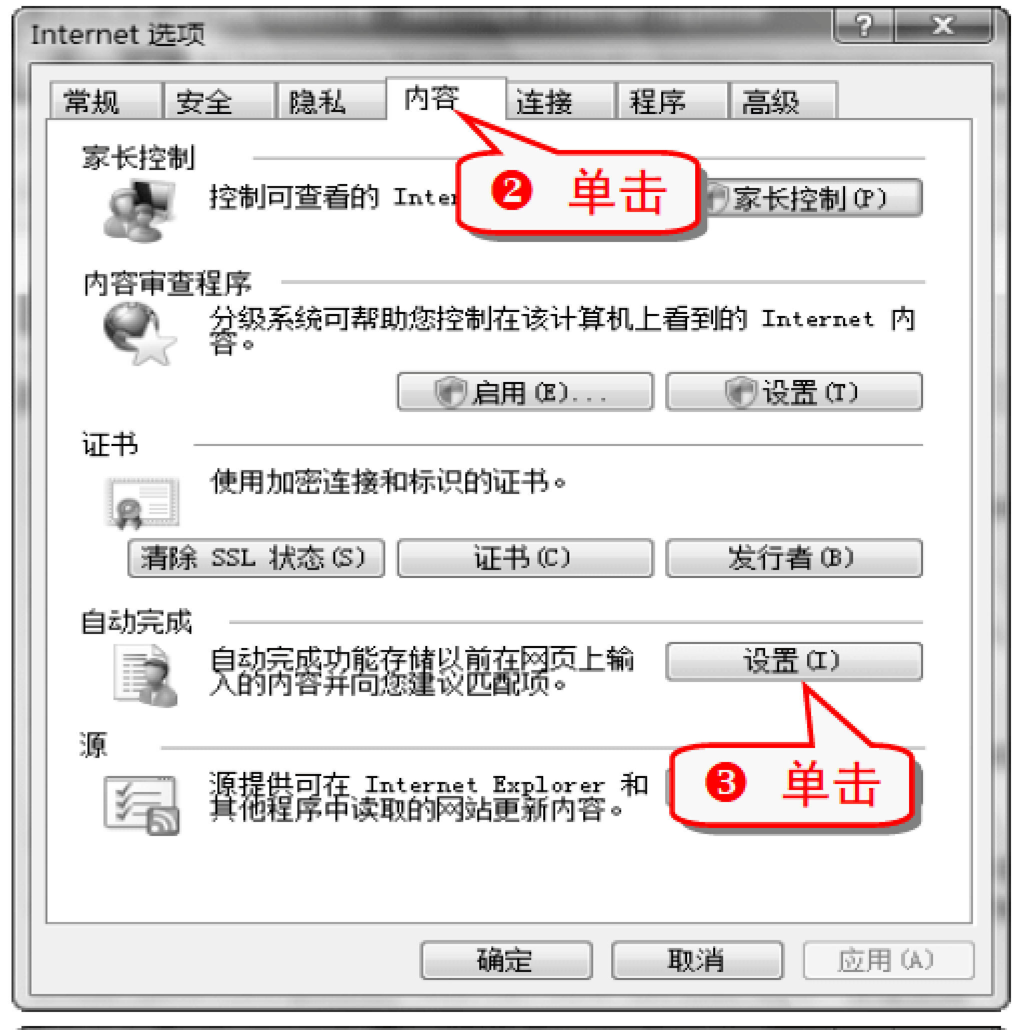


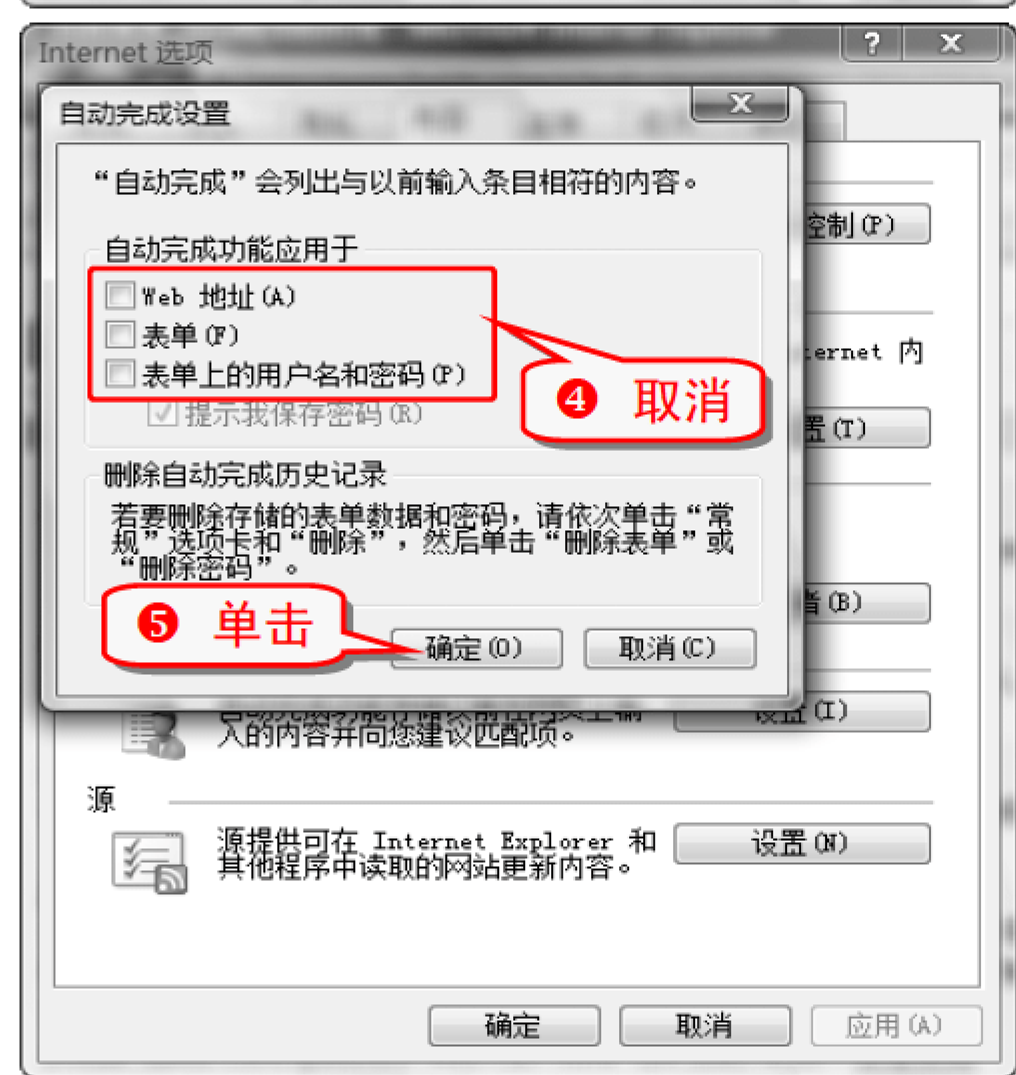
技巧155　防止上网所填信息被泄露

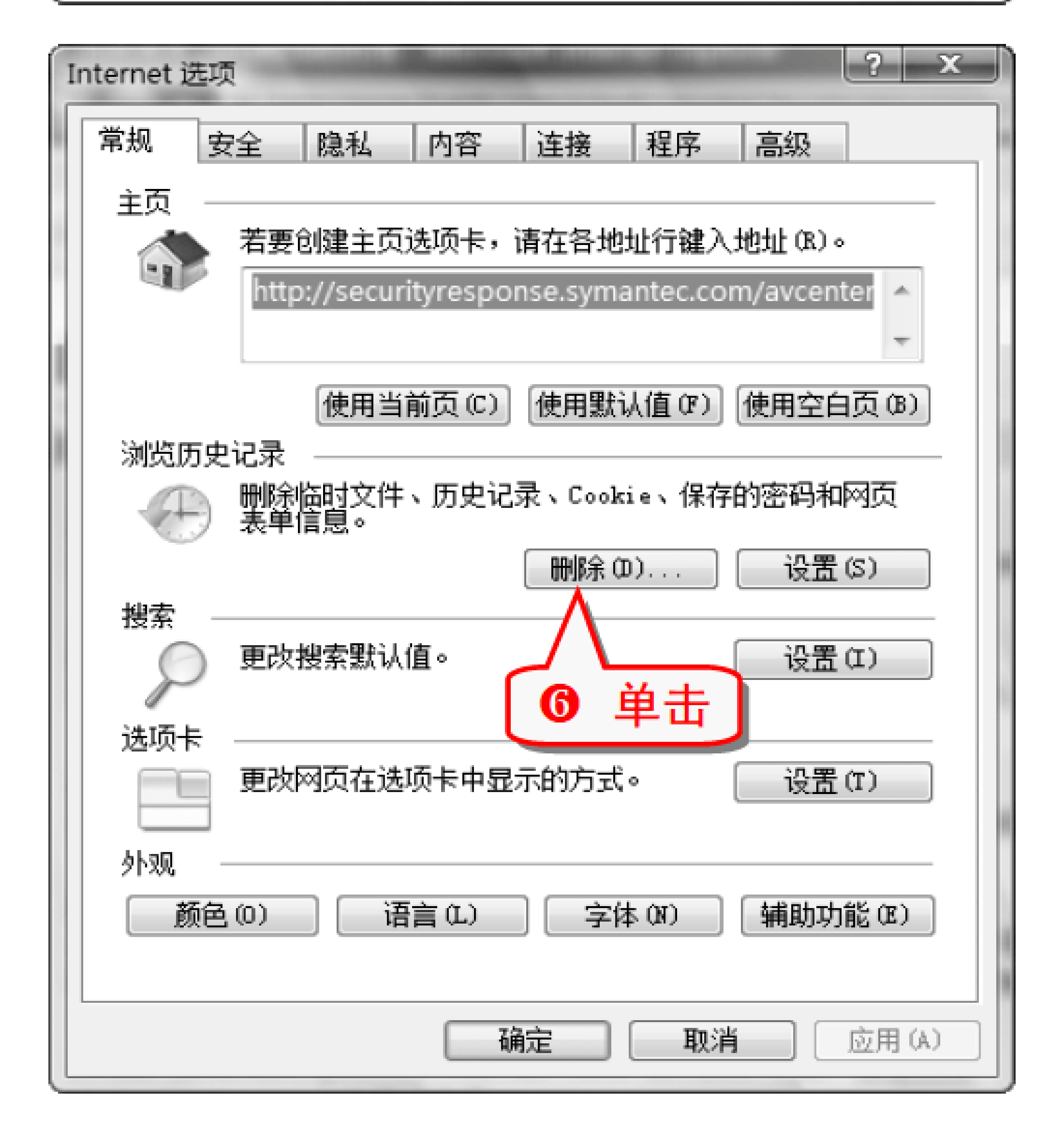
用户可以通过“自动完成”功能解决上网浏览时所填写的信息被泄露的安全问题。

❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令。









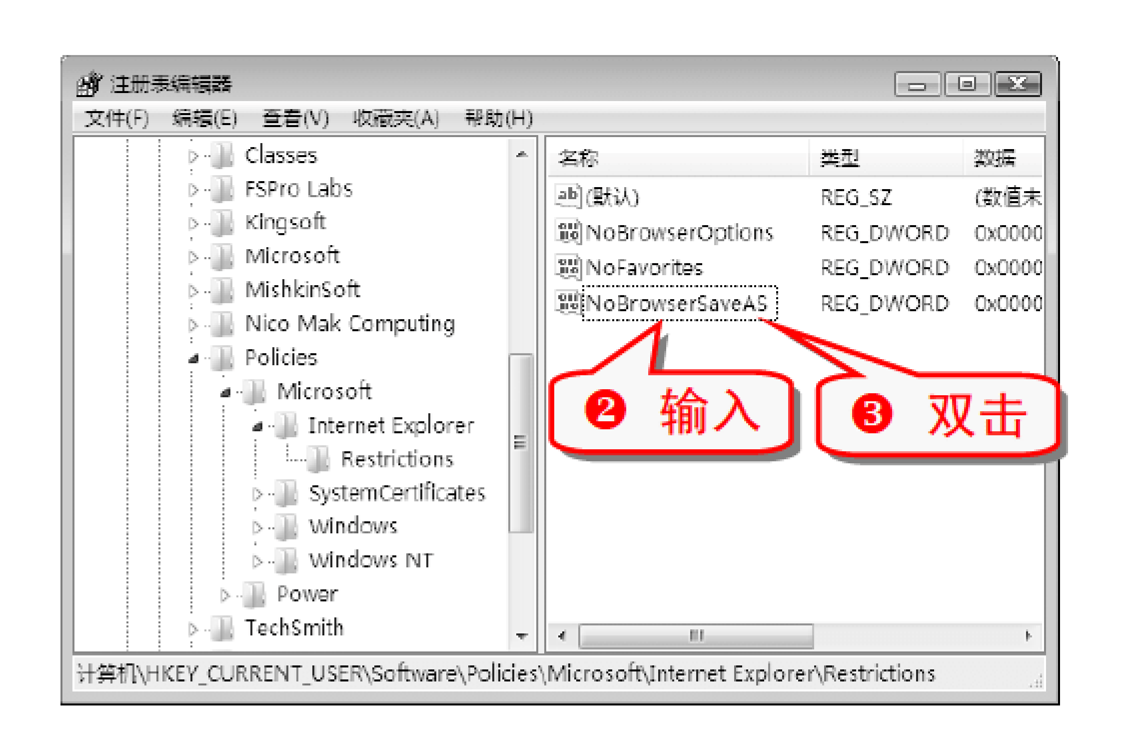


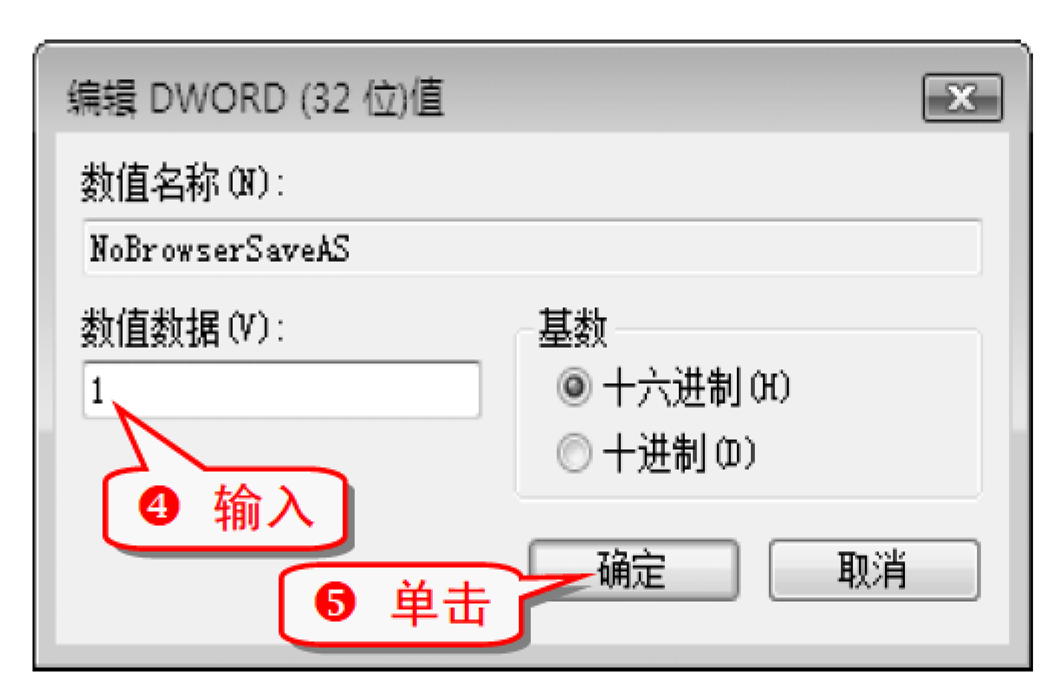
❼ 单击“删除表单”按钮将表单数据删除，单击“删除密码”按钮将密码删除。

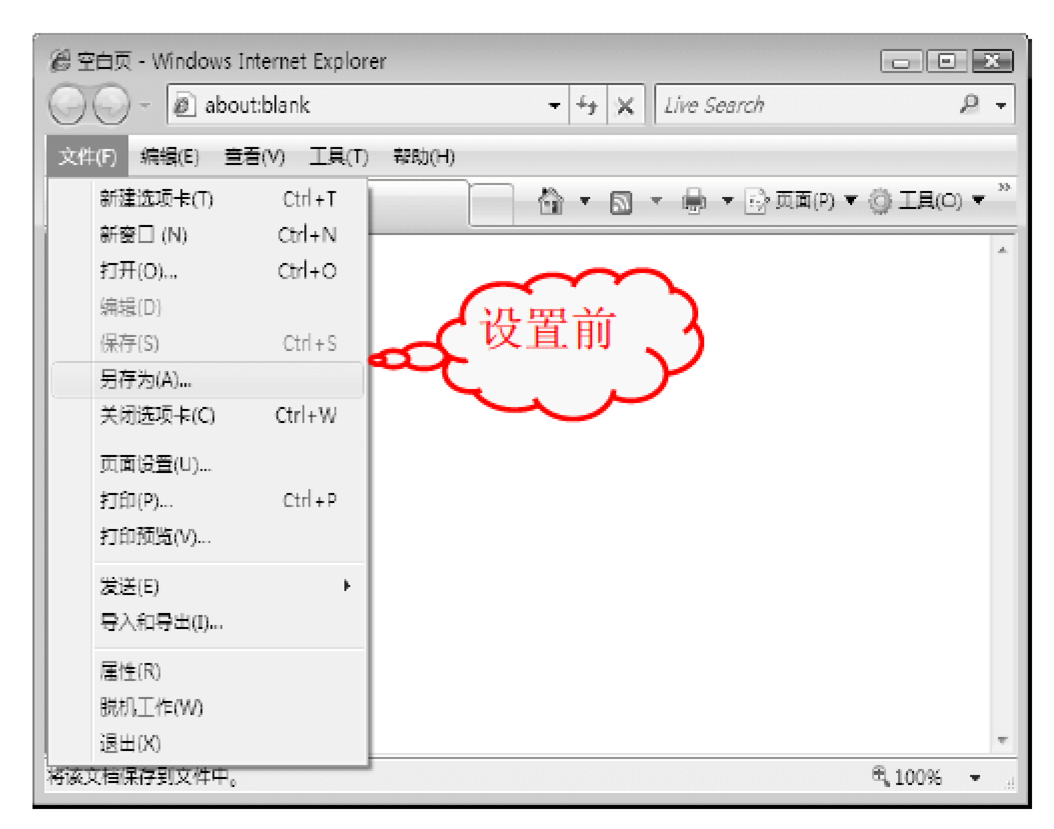
技巧156　禁止保存网页

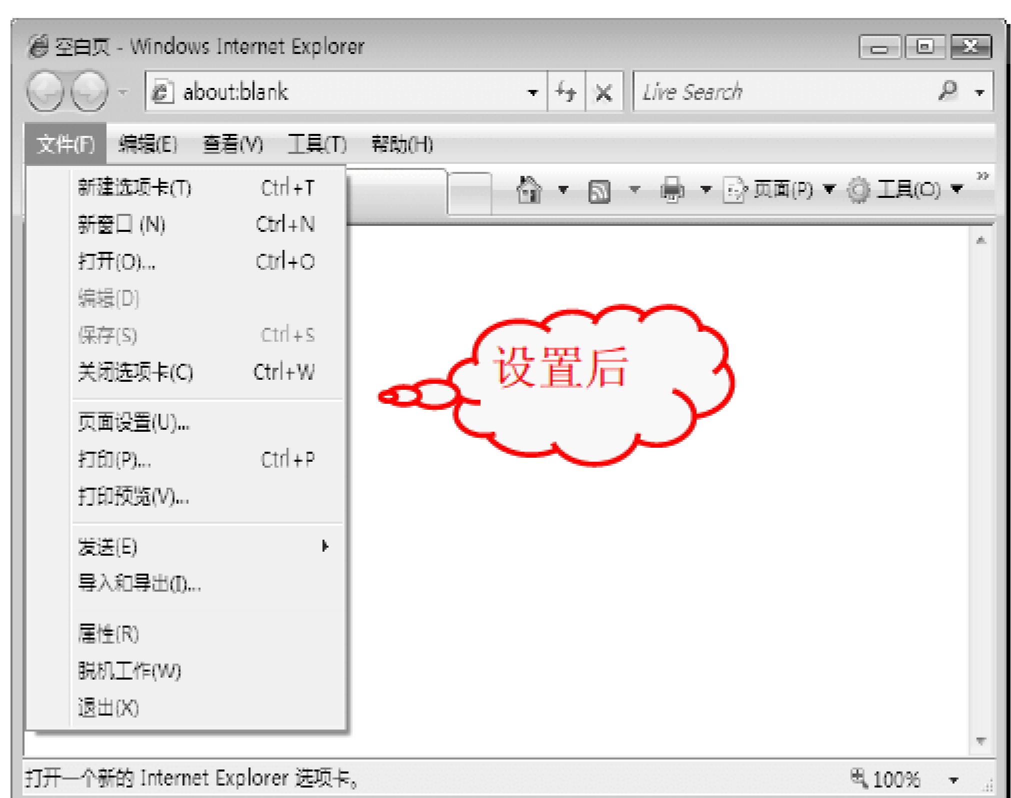
禁用 IE 中的“文件”→“另存为”命令，可以禁止将网页内容保存到硬盘或网络共享上。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions 分支，新建一个类型为 DWORD(32 位)的键值项。









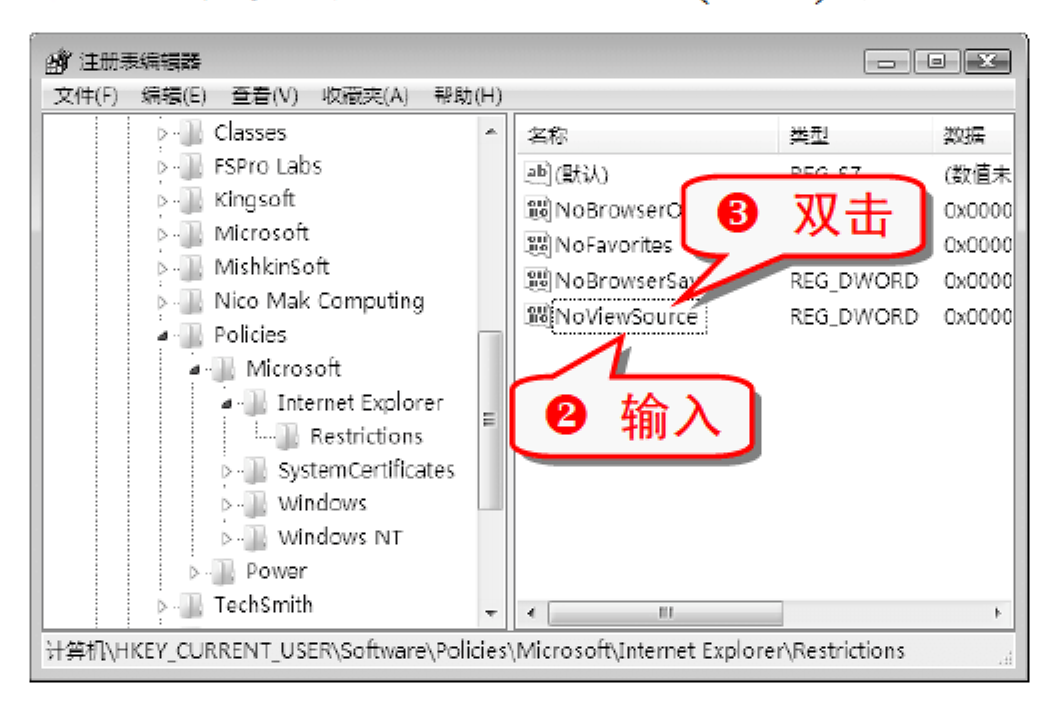
注 意 事 项

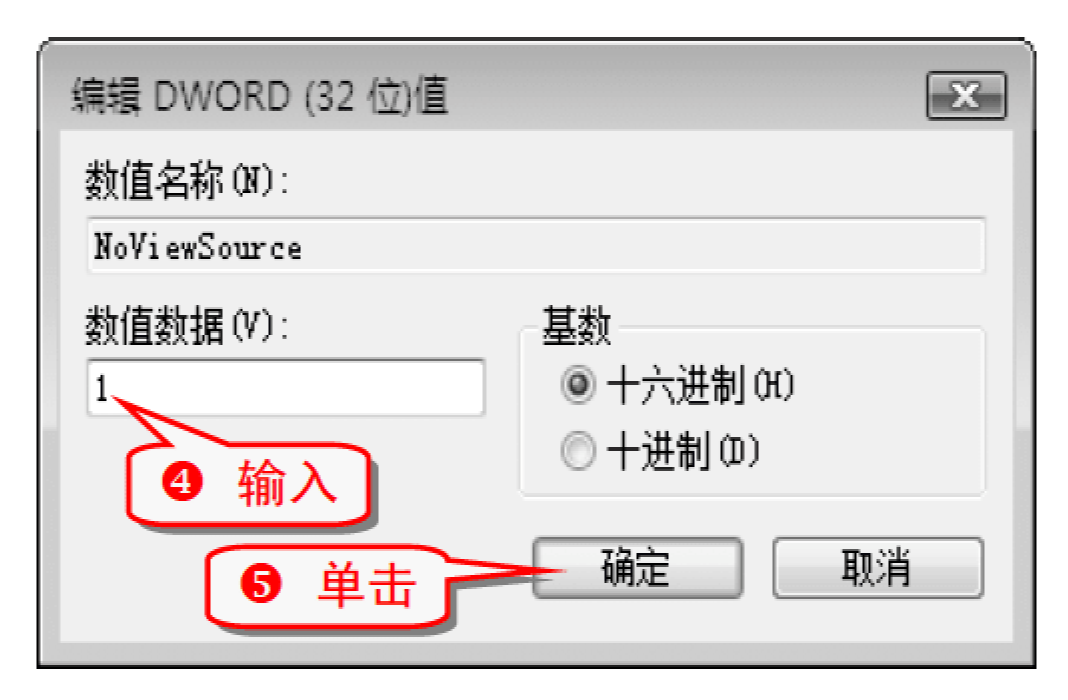
将 NoBrowerSaveAS 的键值设置为 0 即可启用"文件"→"另存为"命令。设置在刷新后生效。

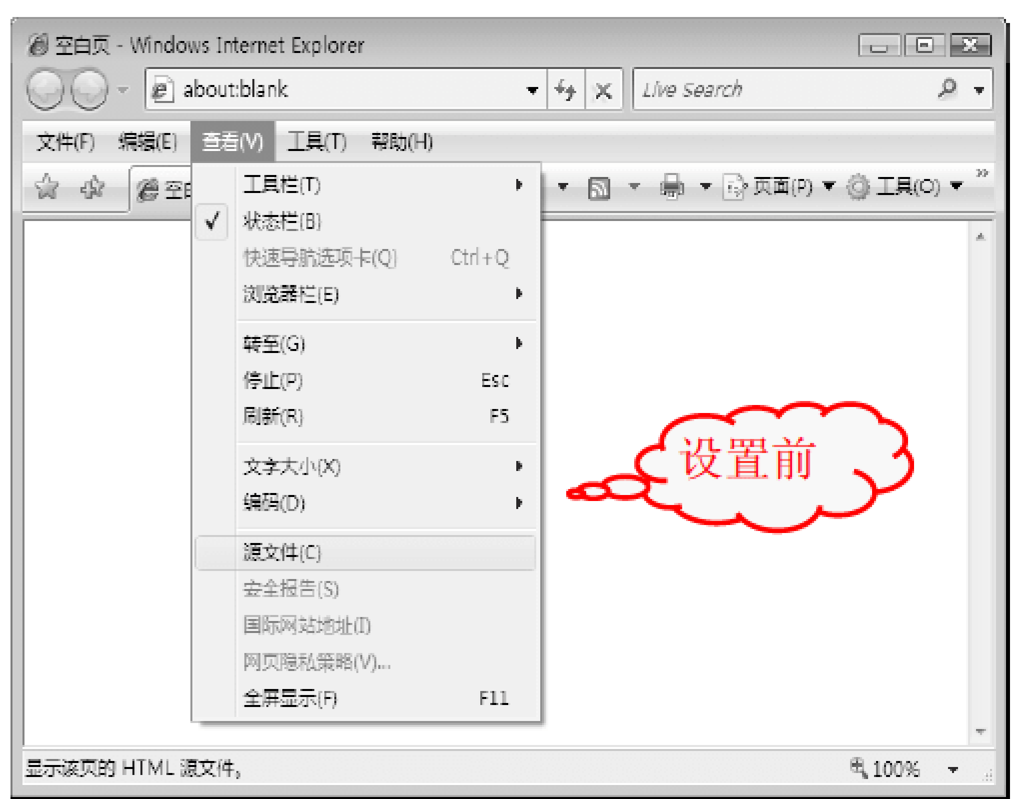
技巧157 禁止查看网页的源文件

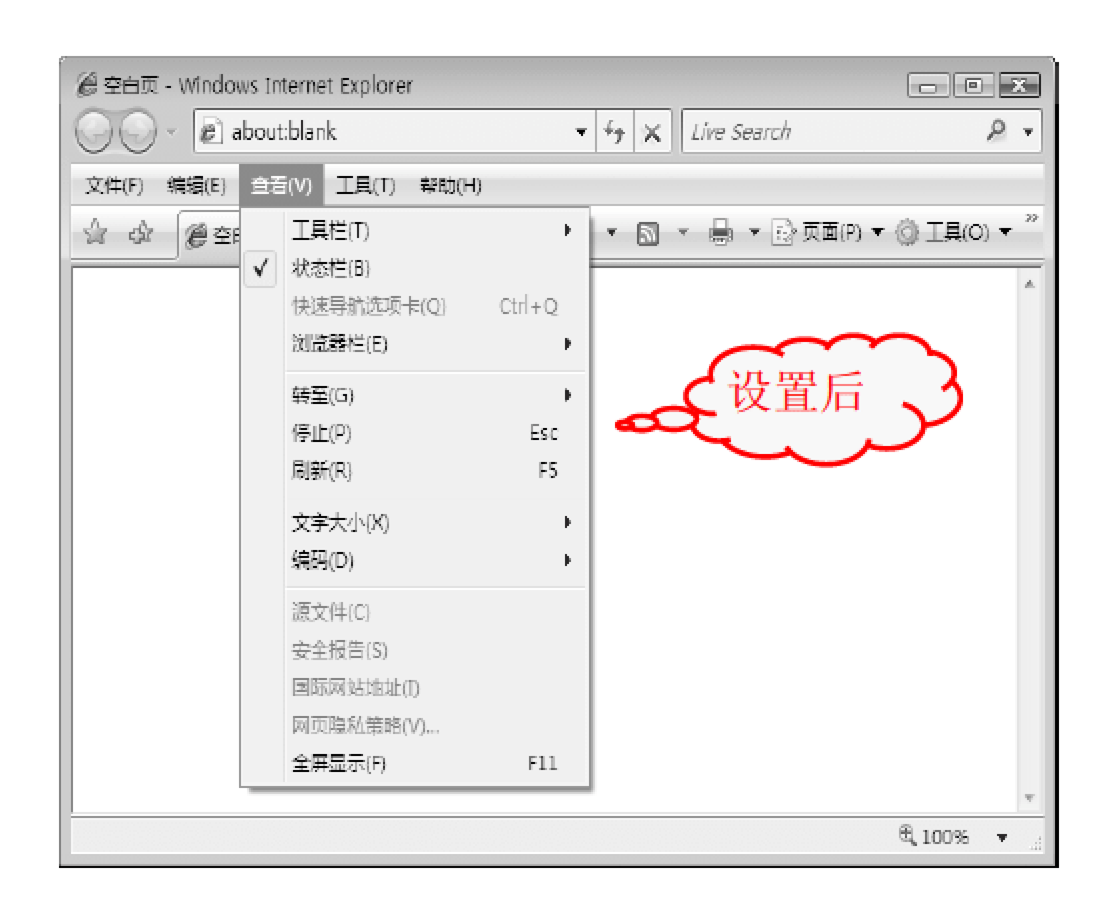
如果不想其他用户查看网页的源文件，可以通过修改注册表将该功能禁用。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions 分支，新建一个类型为 DWORD(32 位)的键值项。









注 意 事 项

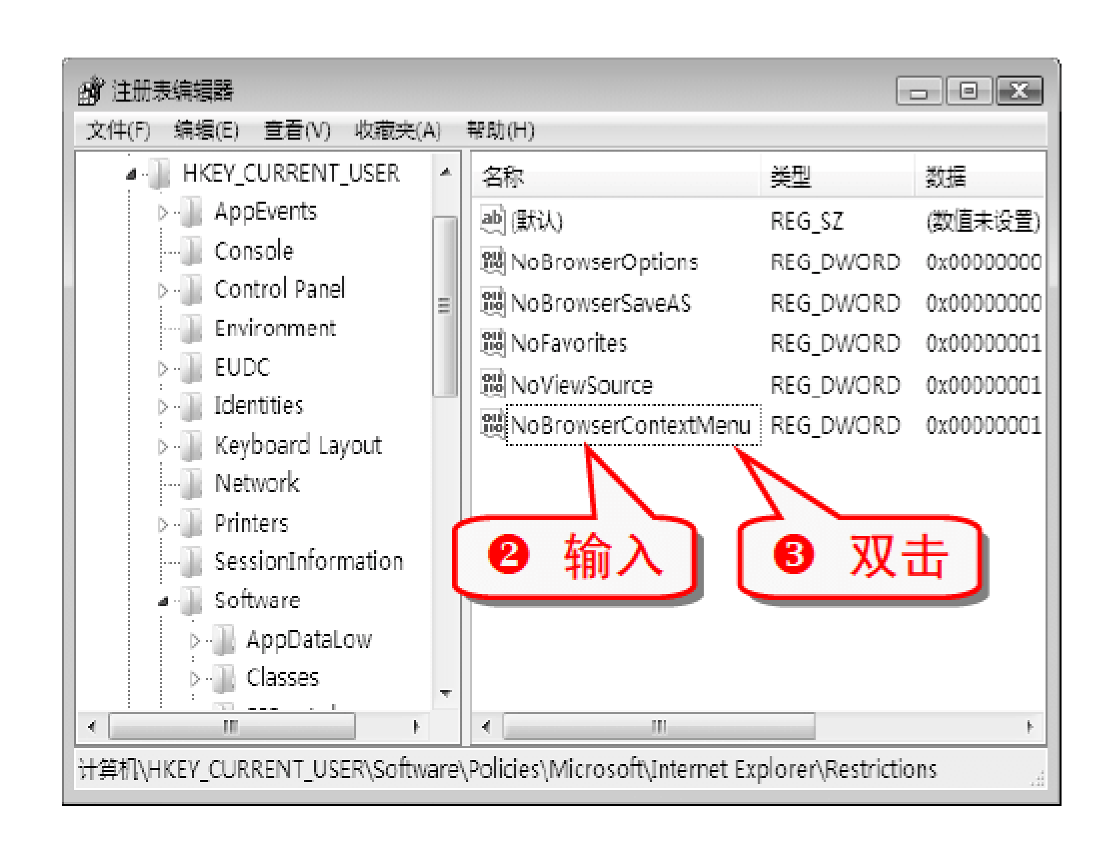
将 NoViewSource 的键值设置为 0 即可启用查看源文件的功能。设置在刷新后生效。

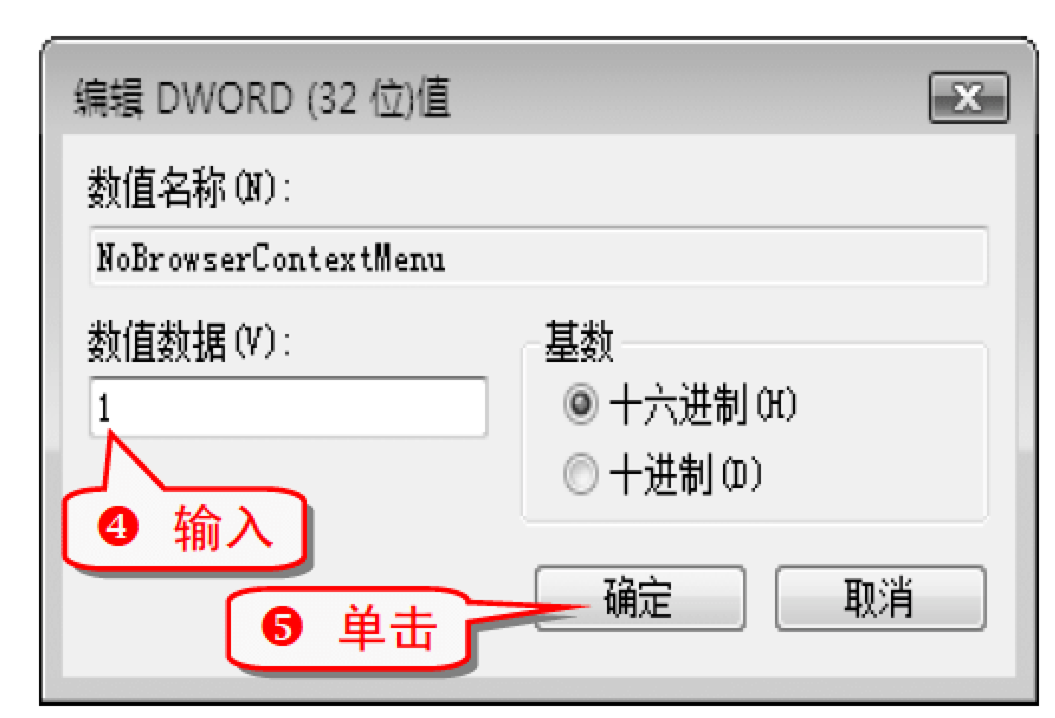
技巧158 在 IE 中禁止使用鼠标右键

如果不想让别的用户使用右键菜单保存网页中的图片或文字，可以设置在 IE 中禁用鼠标右键。通过修改注册表可以禁用在 IE 中的右击功能。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions 分支，新建一个类型为 DWORD(32 位)的键值项。







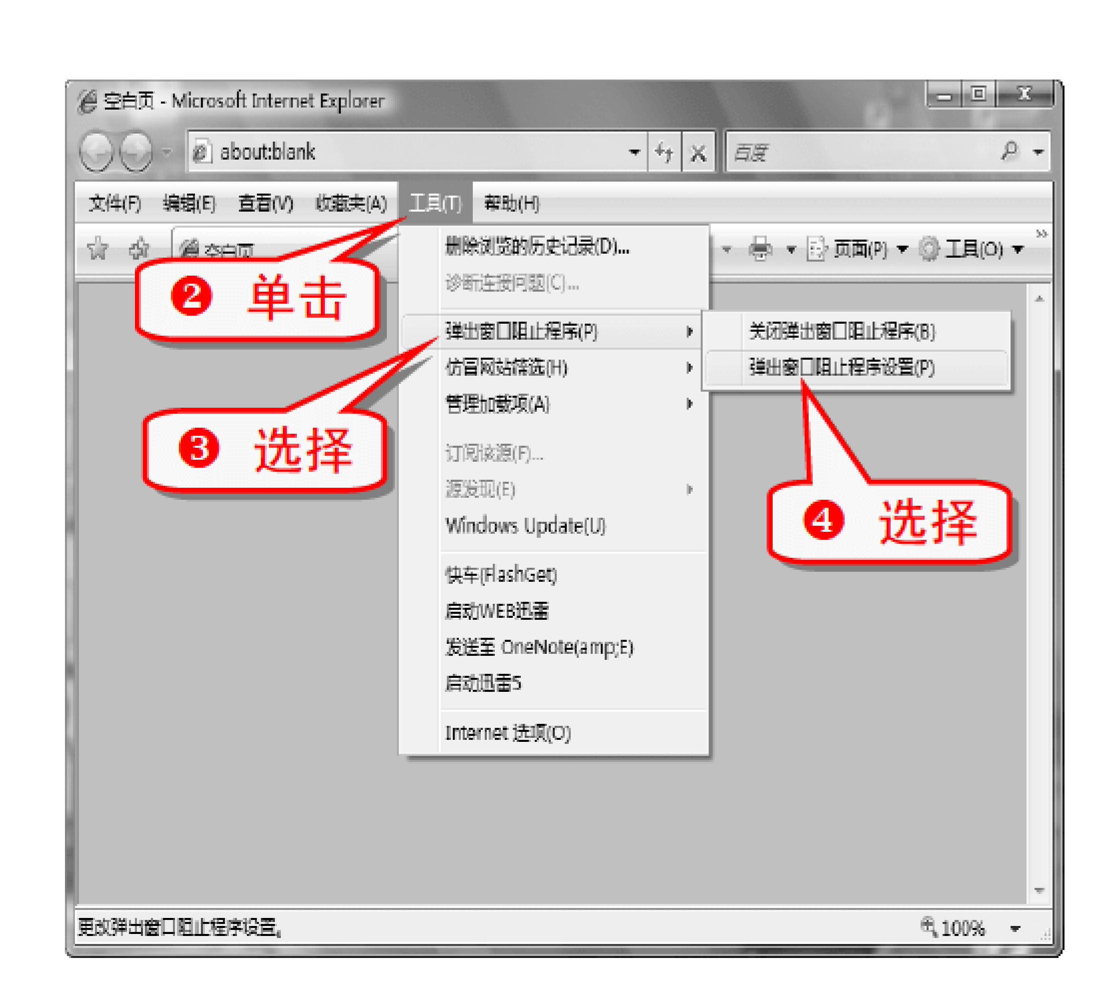
注　意　事　项

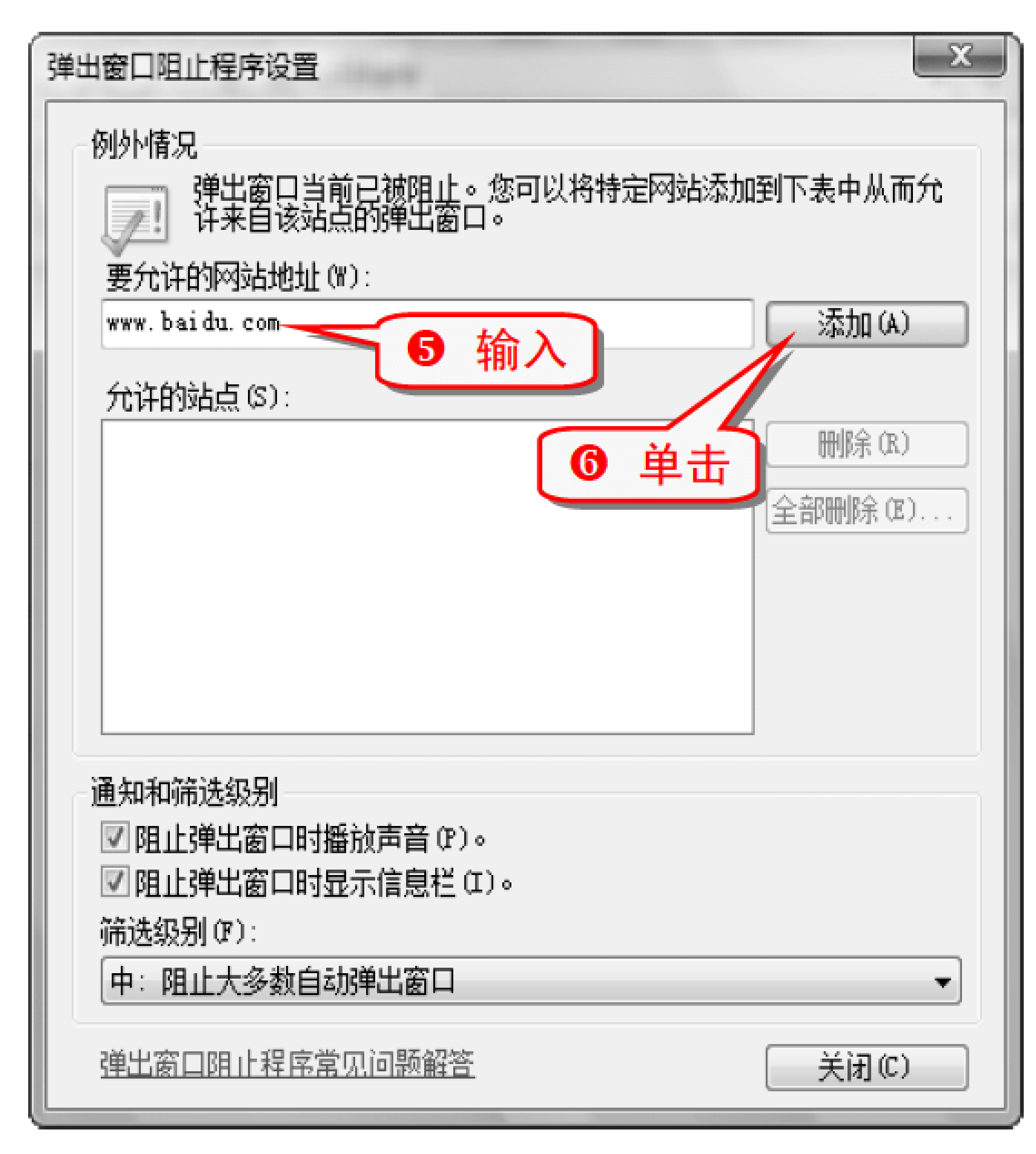
将 NoBrpwserContextMenu 的键值设置为 0，即可启用 IE 中的右击功能。设置在刷新后生效。

技巧159　屏蔽 IE 的弹出窗口

浏览网页时，有时会受到不断弹出的广告窗口的困扰，此时，开启屏蔽 IE 弹出窗口的功能可以进行屏蔽。

❶ 打开 IE 浏览器。

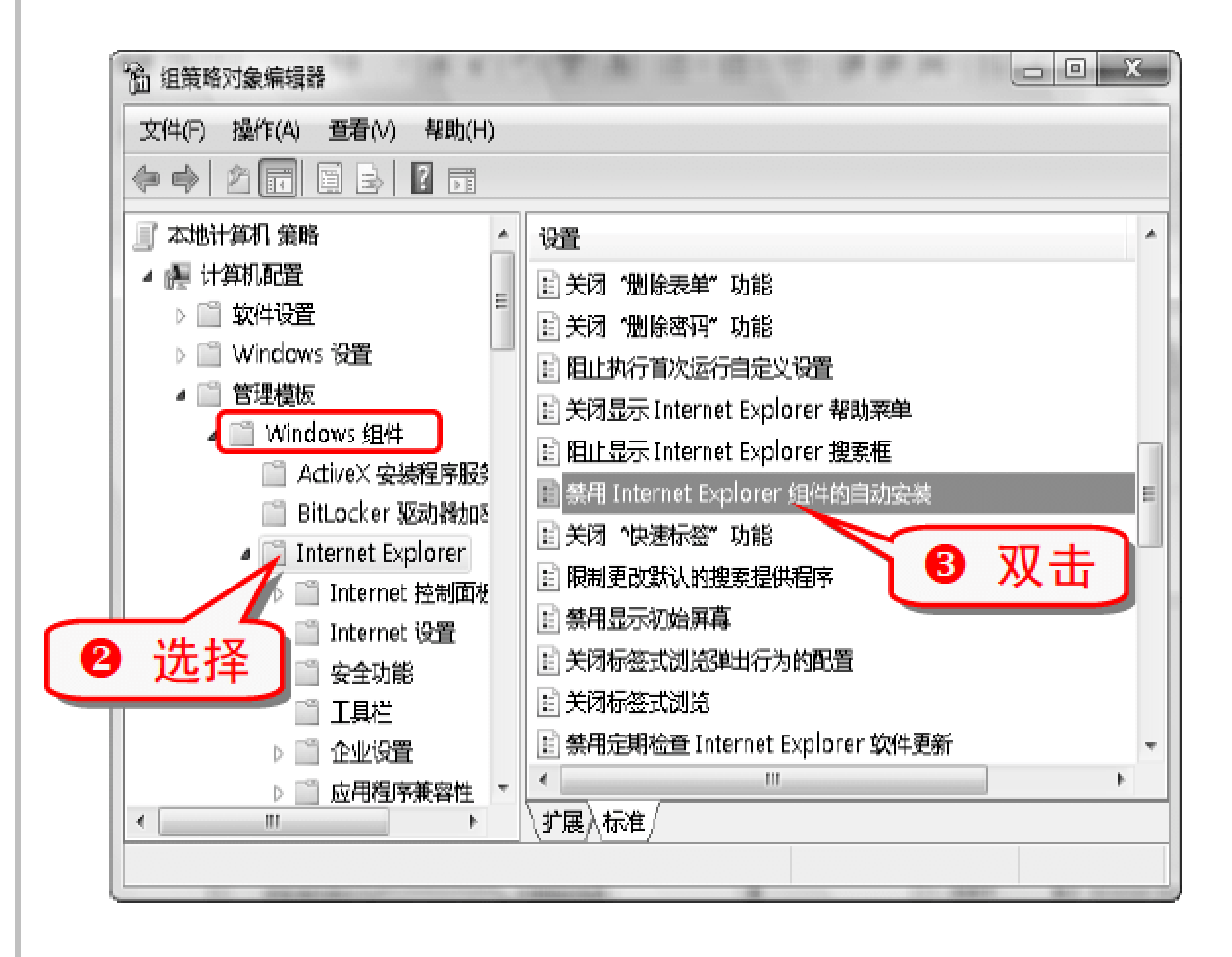


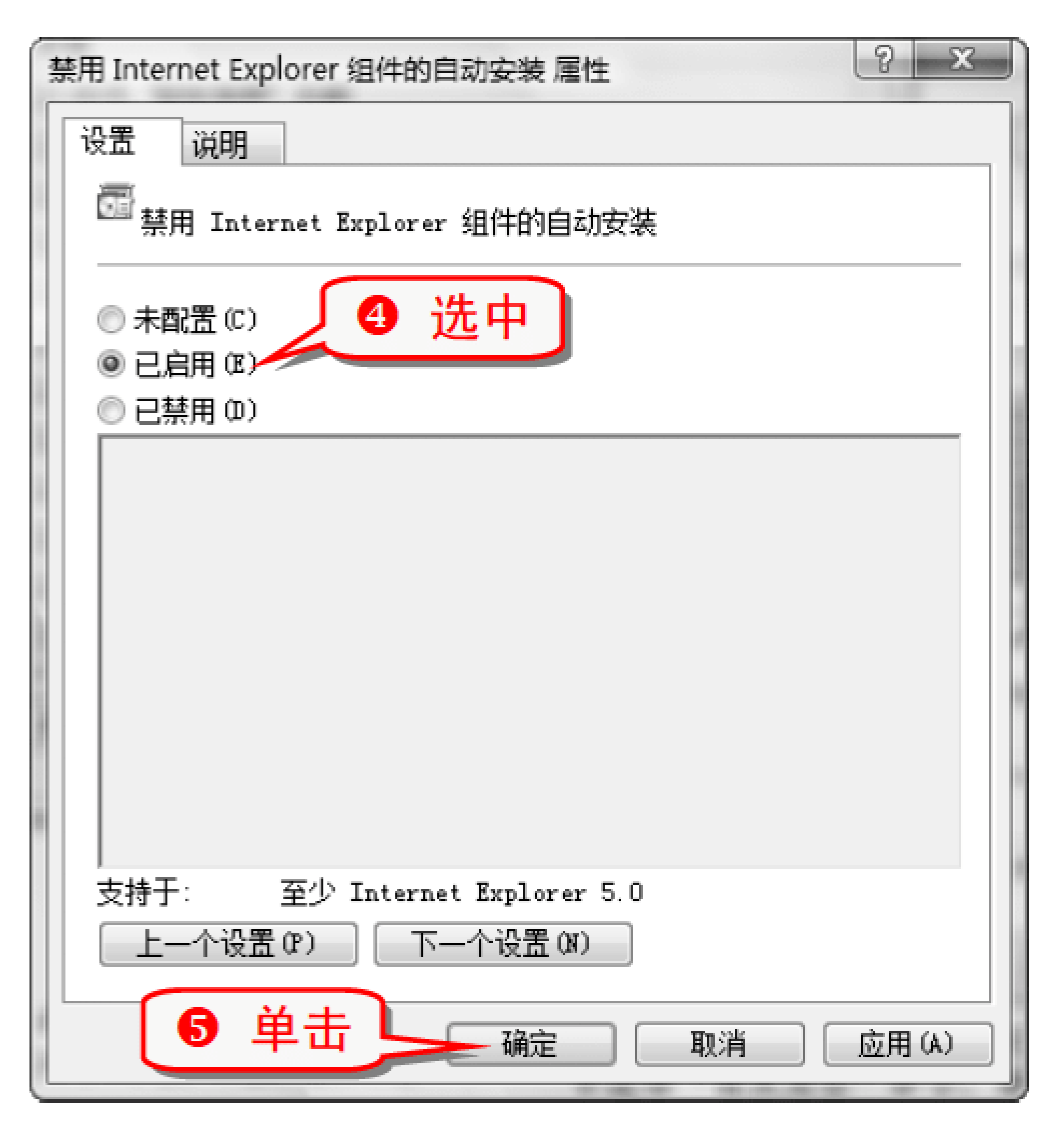


技巧160　解决 IE 插件的提示问题

在浏览网页的过程中，有时会遇到“是否安装 Flash 插件”或者“是否安装 3721 网络实名”这样的提示，通过对“本地计算机策略”中的选项设置，可以让这恼人的提示消失。

❶ 打开组策略对象编辑器，展开“计算机配置”→“管理模版”→“Windows 组件”→Internet Explorer 分支。



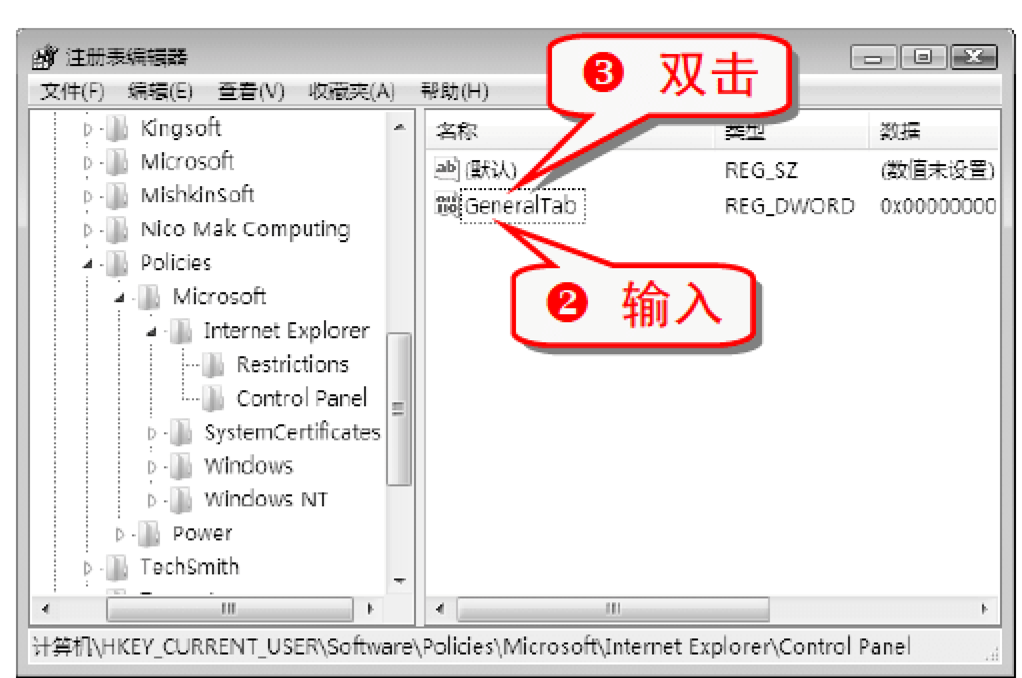


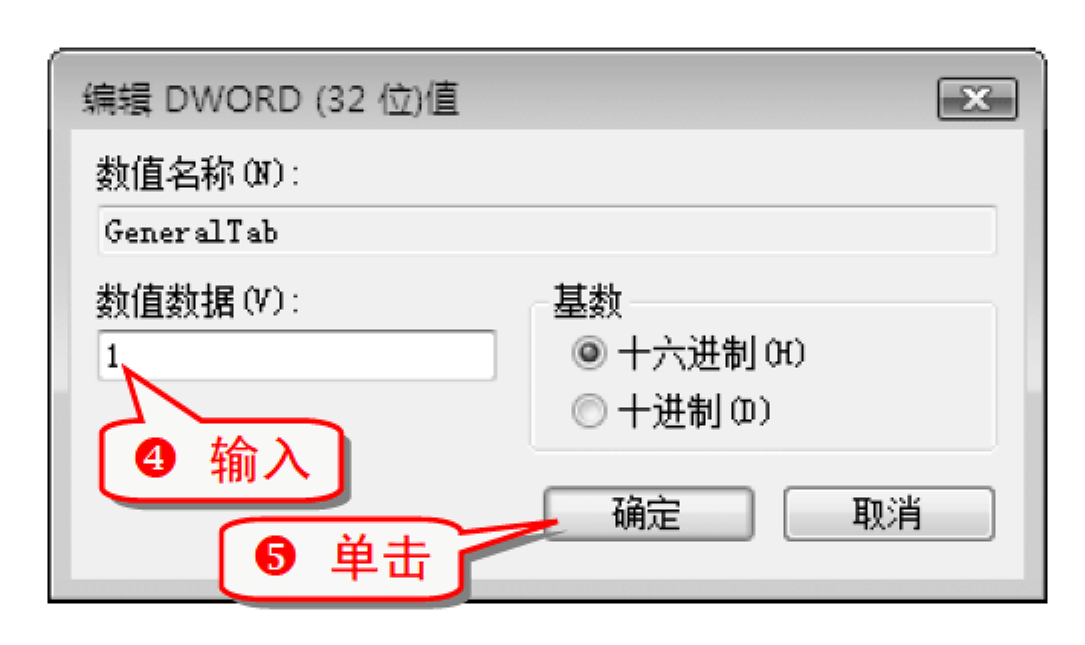
技巧161　禁用 Internet 选项的“常规”选项卡

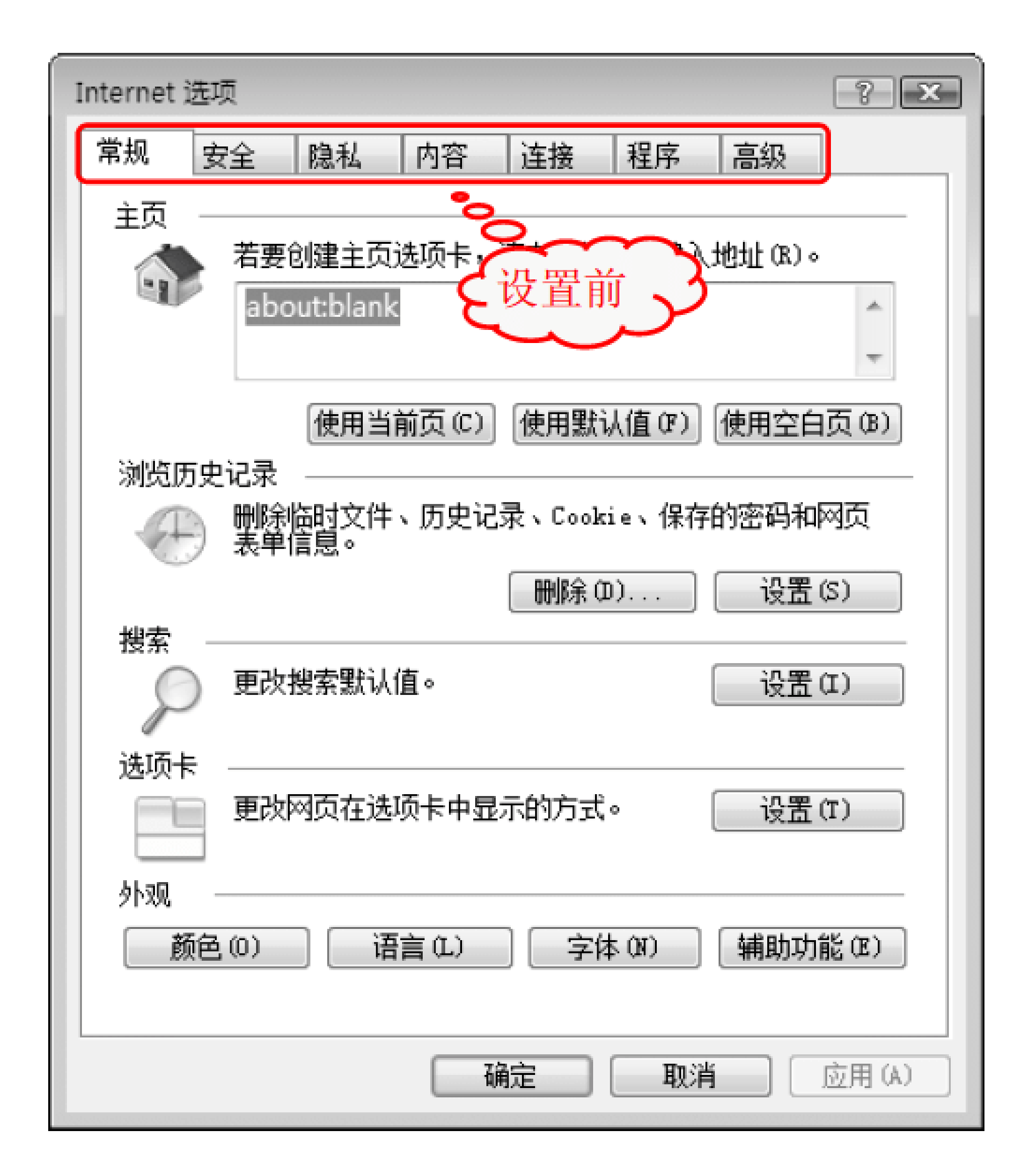
禁用 Internet 选项的“常规”选项卡可以有效防止其他用户恶意修改主页等不安全操作。

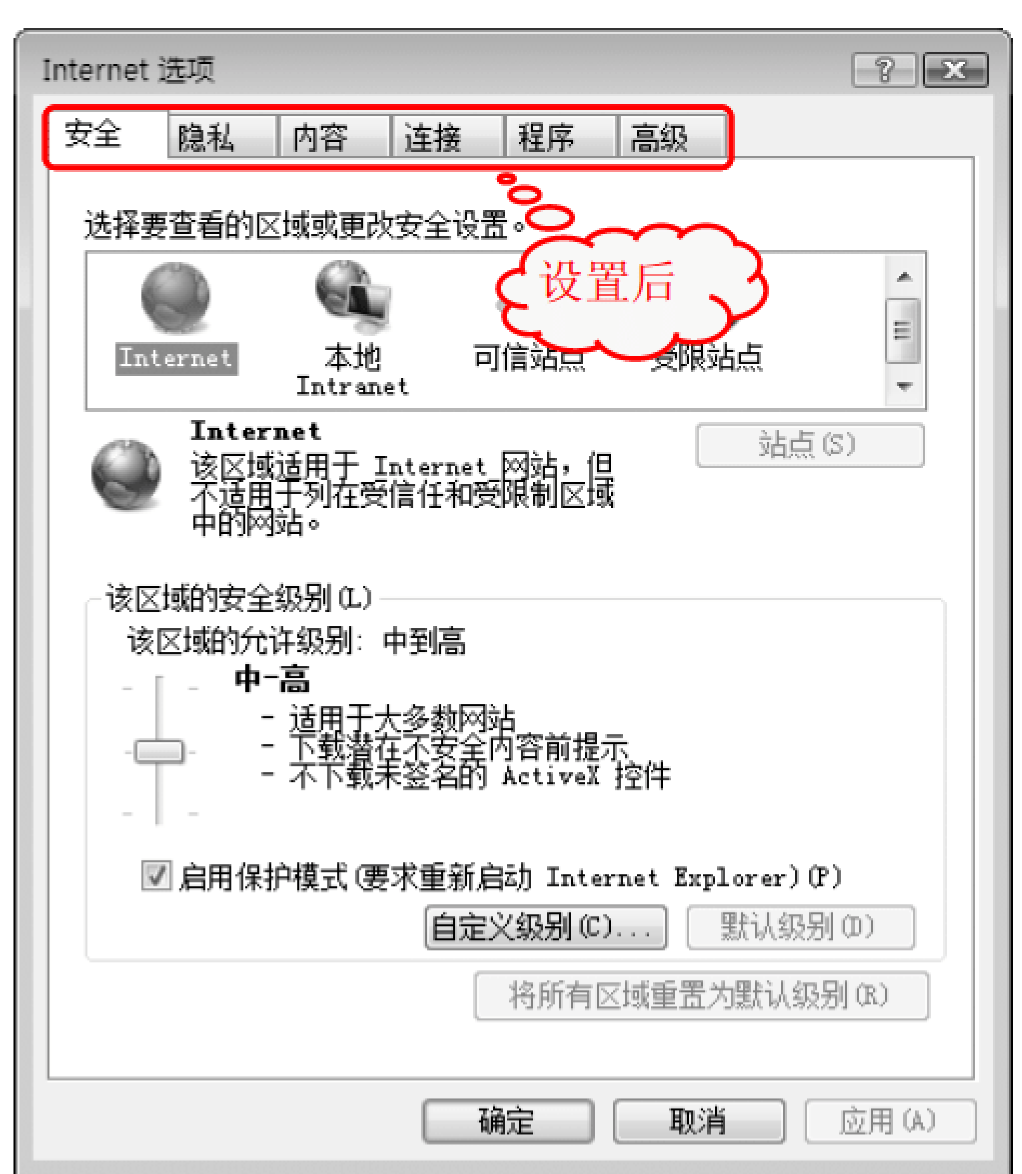
通过以下操作可以禁用 Internet 选项的“常规”选项卡。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel 分支，如果没有 Control Panel 选项则新建一个项，再新建一个类型为 DWORD(32 位)的键值项。









注　意　事　项

将 GeneralTab 的键值设置为 0 即可让“常规”选项卡重新显示出来。设置在刷新后生效。

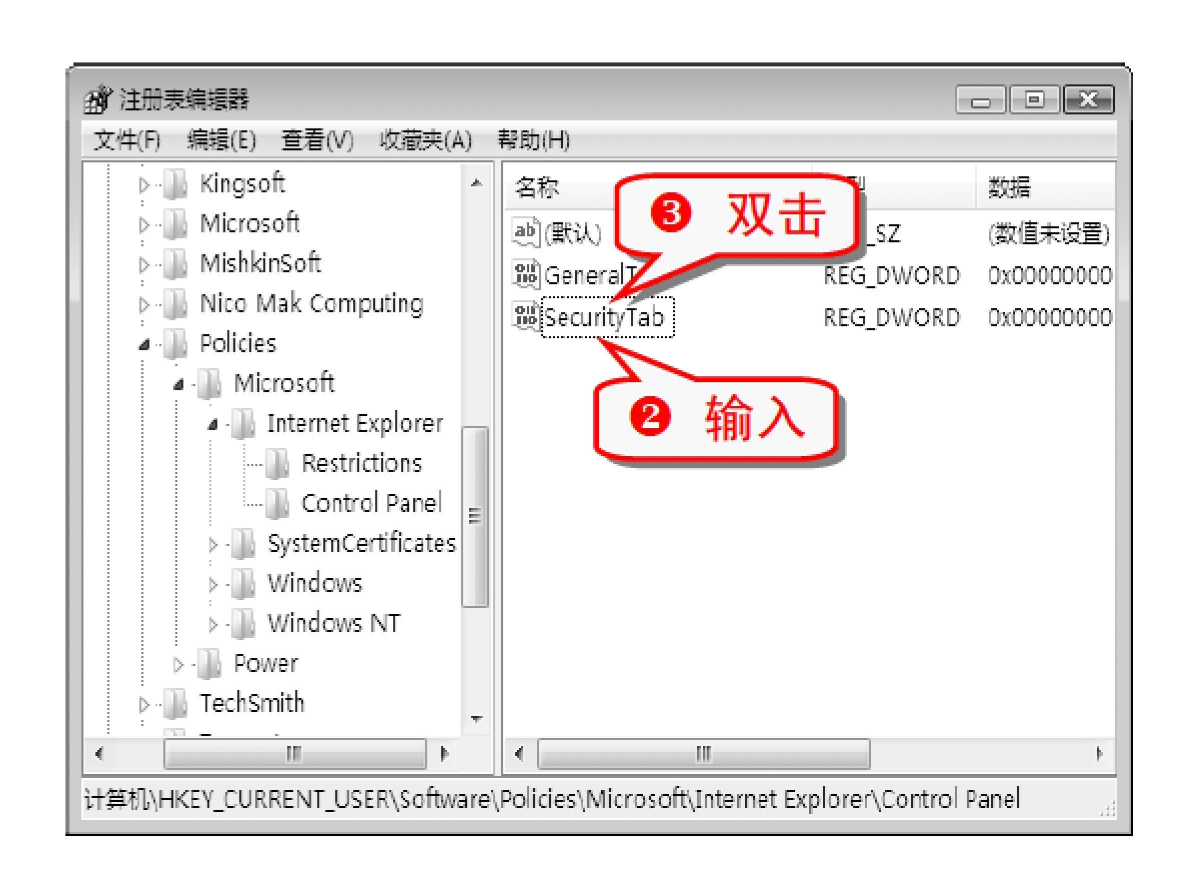
技巧162　禁用 Internet 选项的“安全”选项卡

禁用 Internet 选项的“安全”选项卡，可以防止其他用户随意修改 Web 内容指定的安全设置。

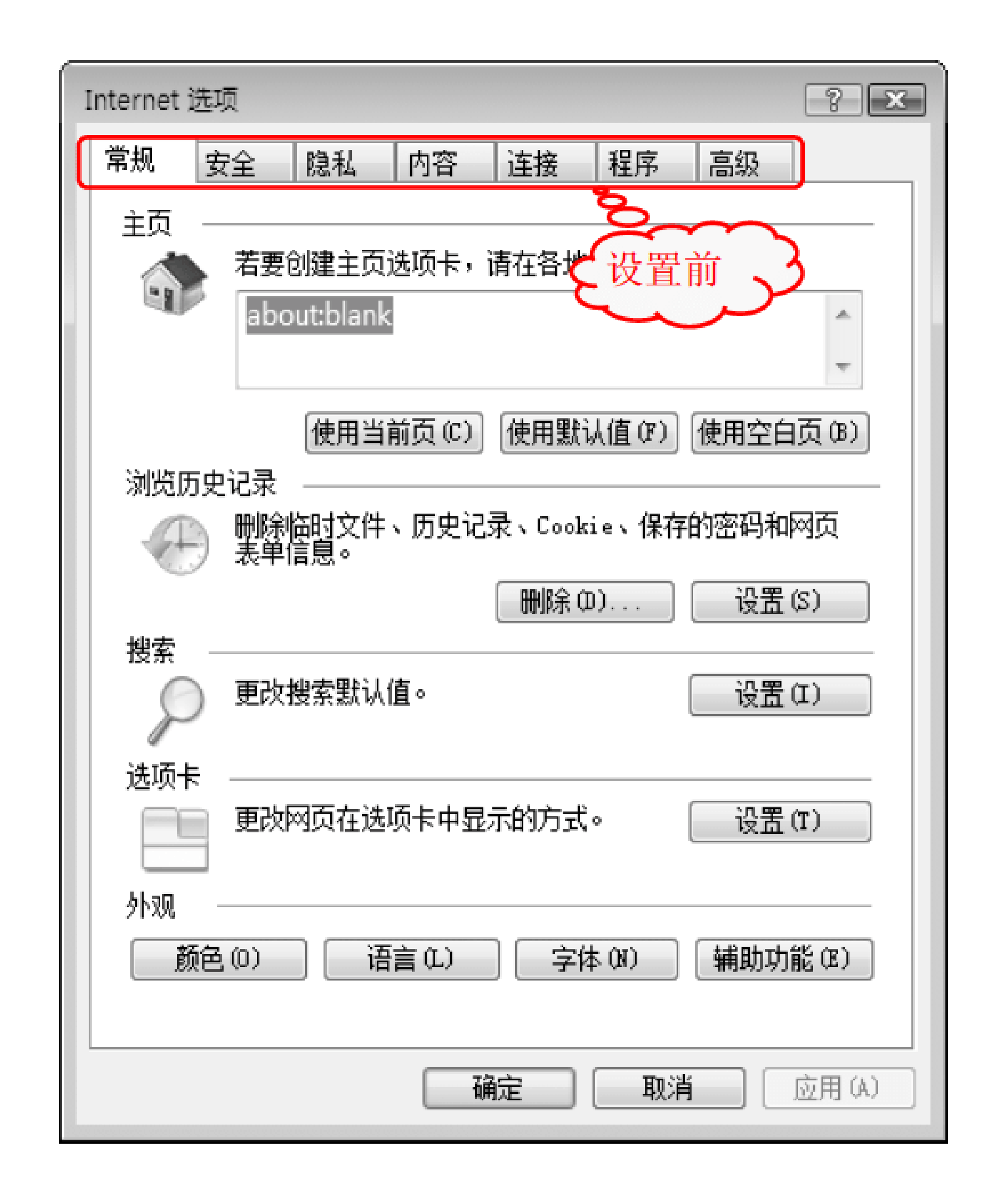
通过以下操作可以禁用 Internet 选项的“安全”选项卡。

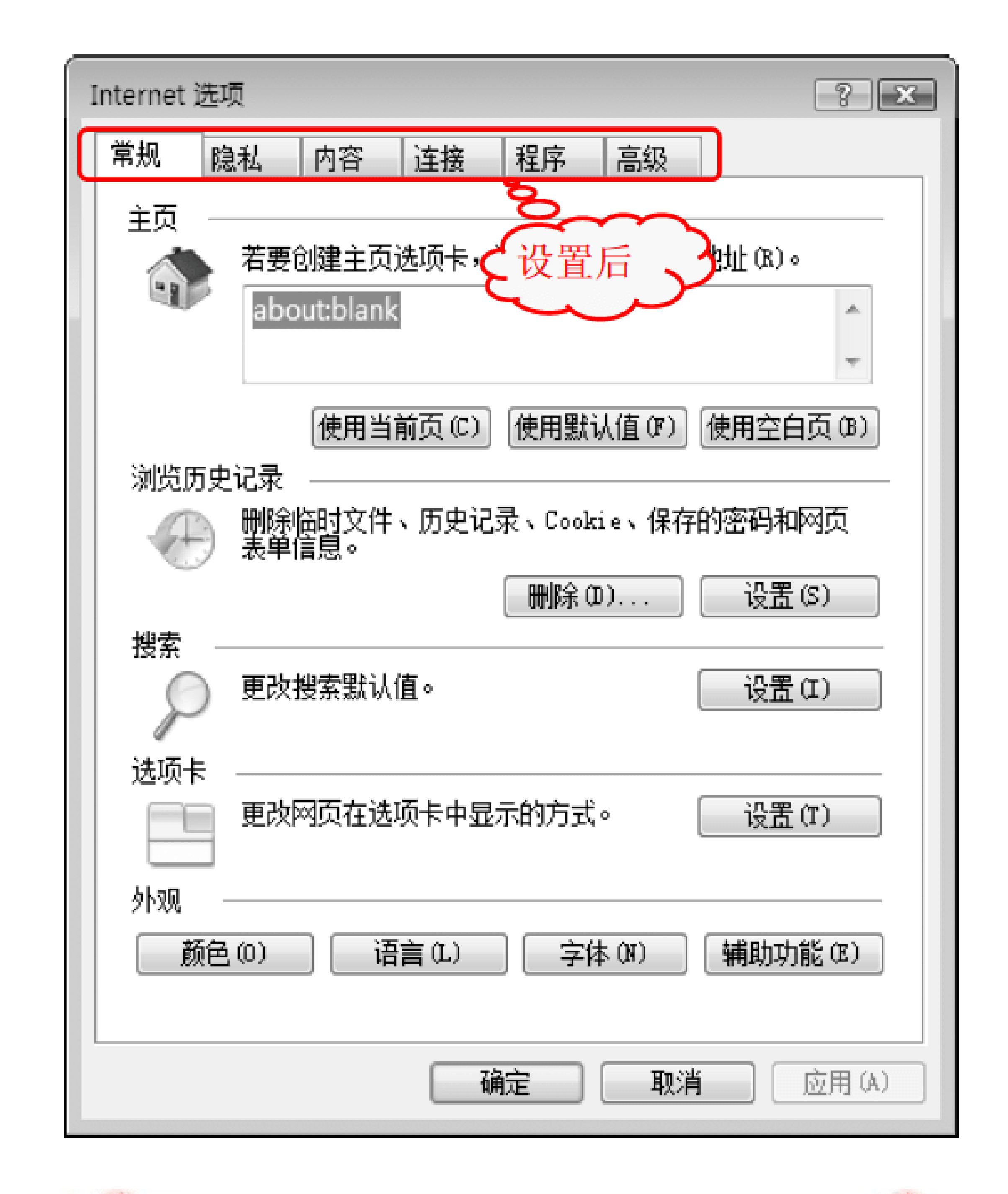


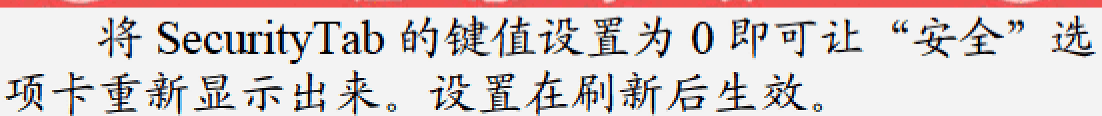
❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\ControlPanel 分支，新建一个类型为 DWORD(32 位)的键值项。











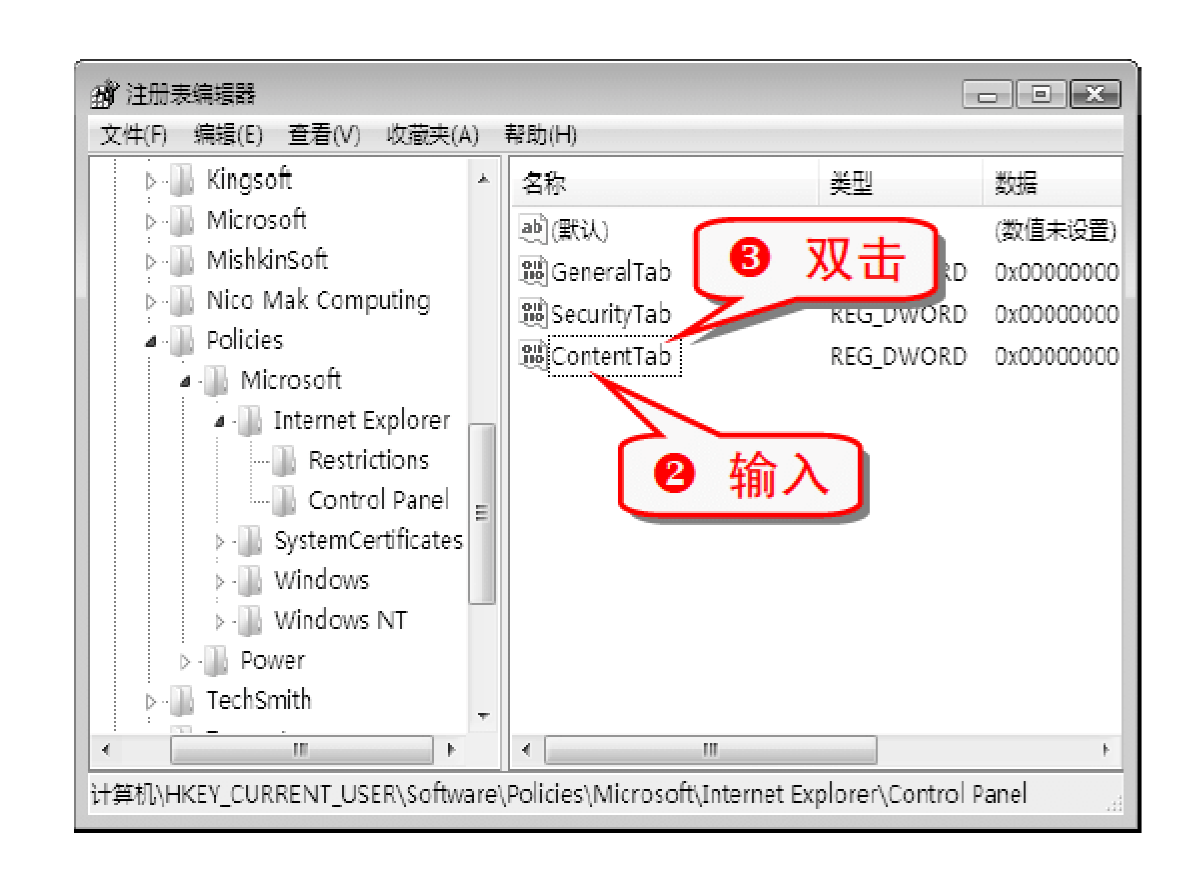
将 SecurityTab 的键值设置为 0 即可让“安全”选项卡重新显示出来。设置在刷新后生效。

技巧163　禁用 Internet 选项的“内容”选项卡

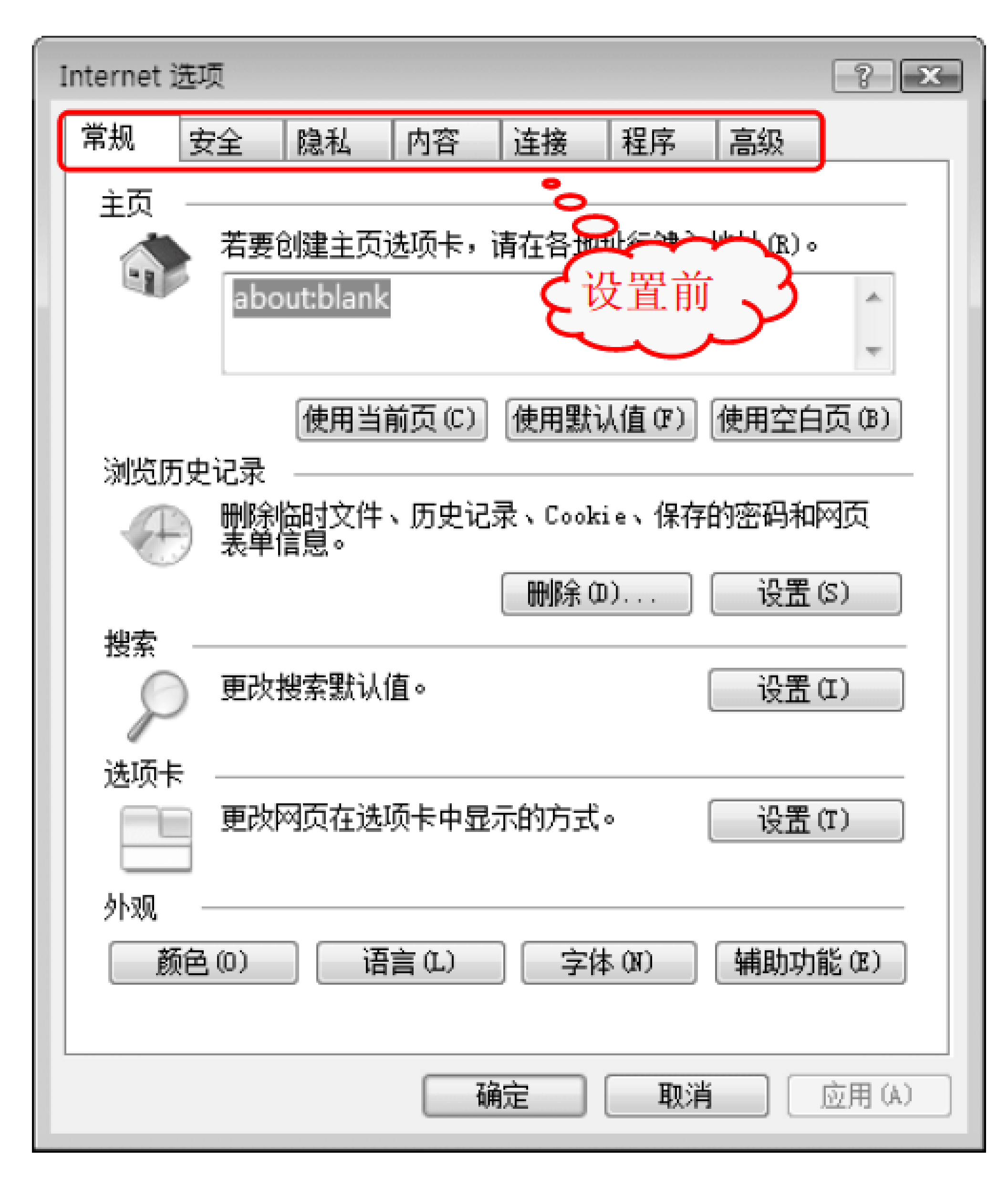
禁用 Internet 选项的“内容”选项卡，可以防止其他用户修改分级审查、证书、个人信息等资料。

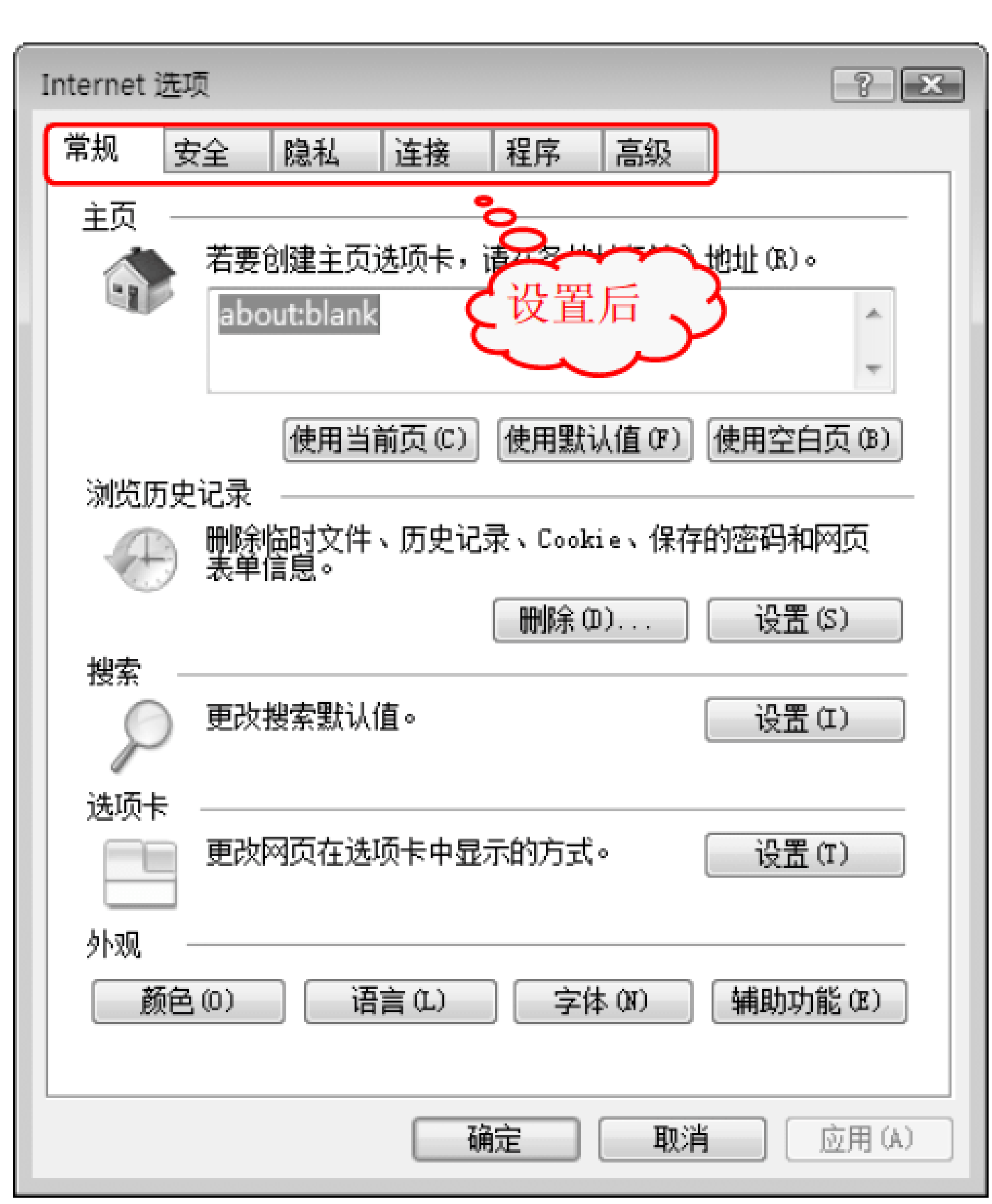
通过以下操作可以禁用 Internet 选项的“内容”选项卡。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel 分支，新建一个类型为 DWORD(32 位)的键值项。











注 意 事 项

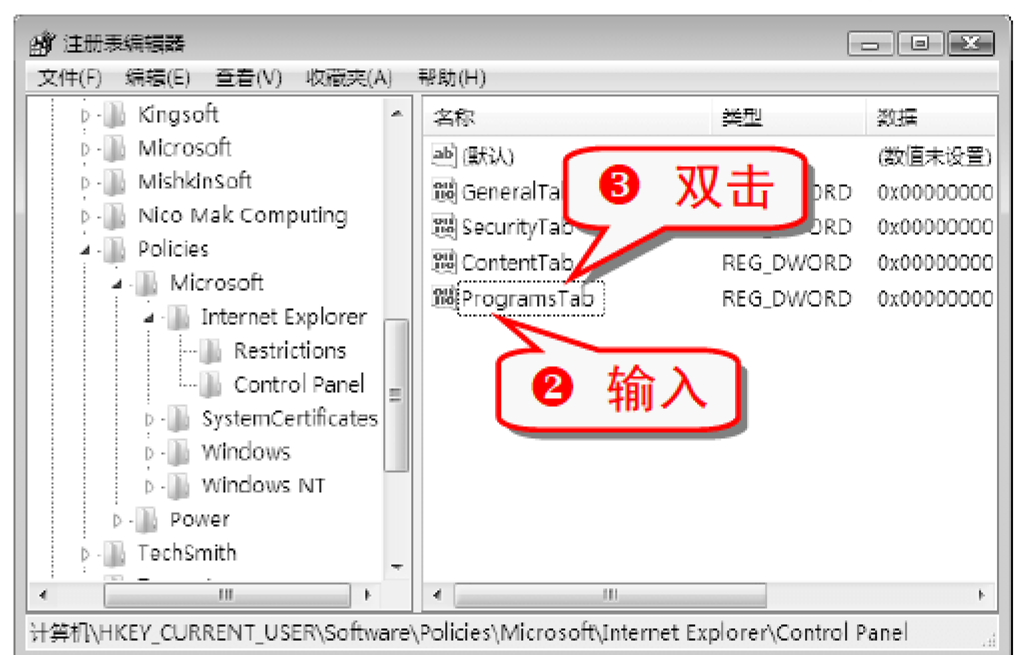
将 ContentTab 的键值设置为 0 即可让“内容”选项卡重新显示出来。设置在刷新后生效。

技巧164 禁用 Internet 选项的“程序”选项卡

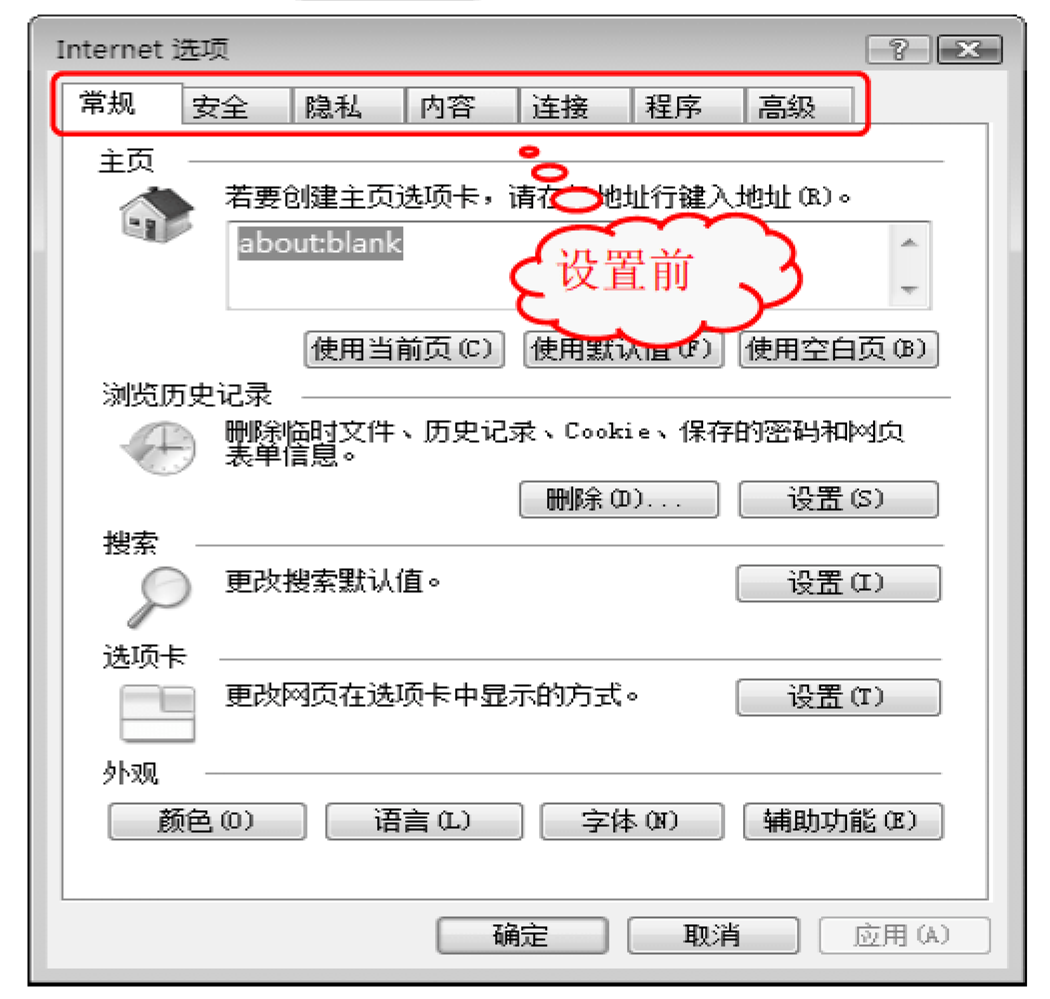
禁用 Internet 选项的“程序”选项卡，可以防止其他用户进行更改 HTML 编辑器、电子邮件等信息、重置 Web 设置等操作。

通过以下操作可以禁用 Internet 选项的“程序”选项卡。

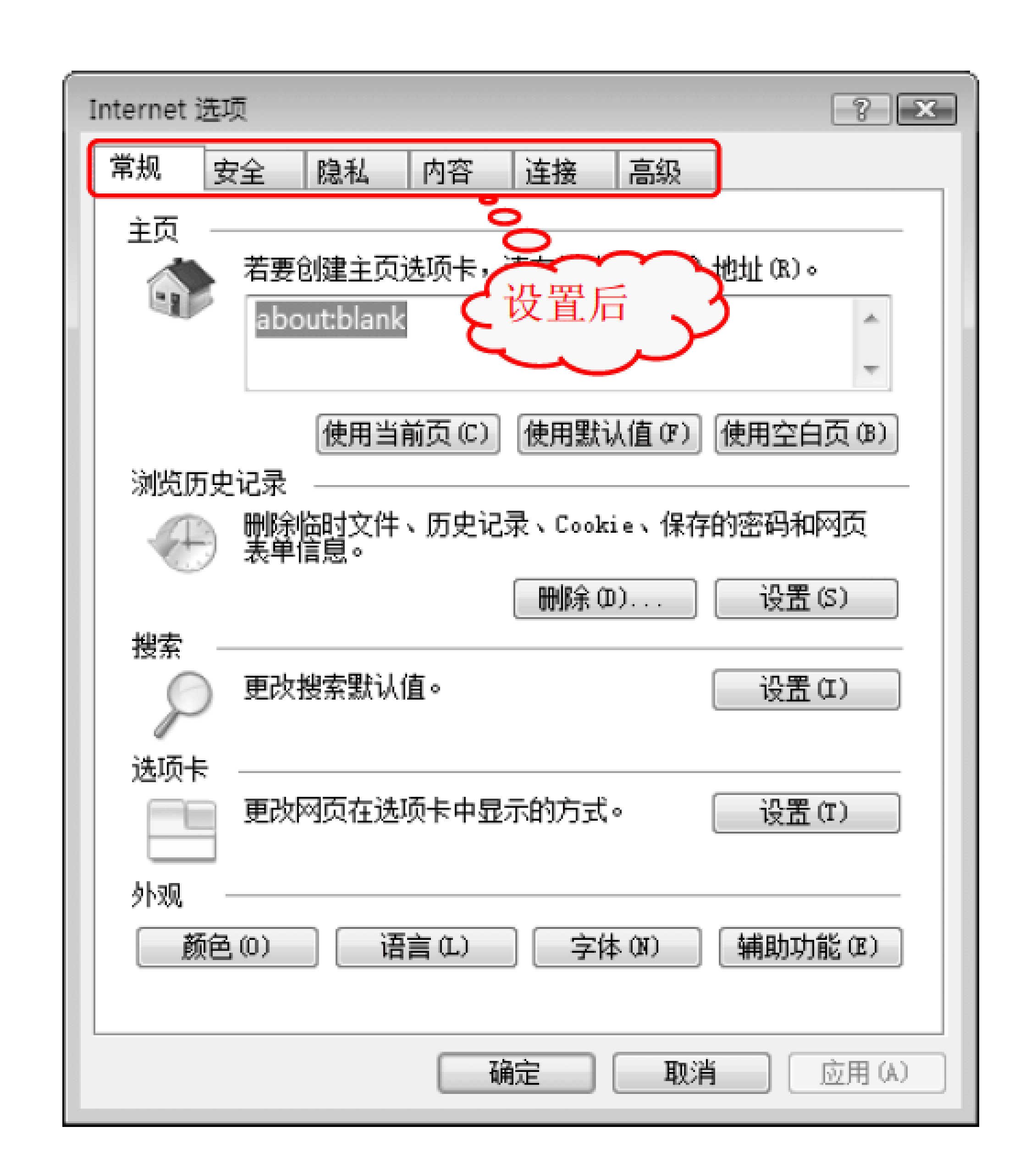
❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel 分支，新建一个类型为 DWORD(32 位)的键值项。











注　意　事　项

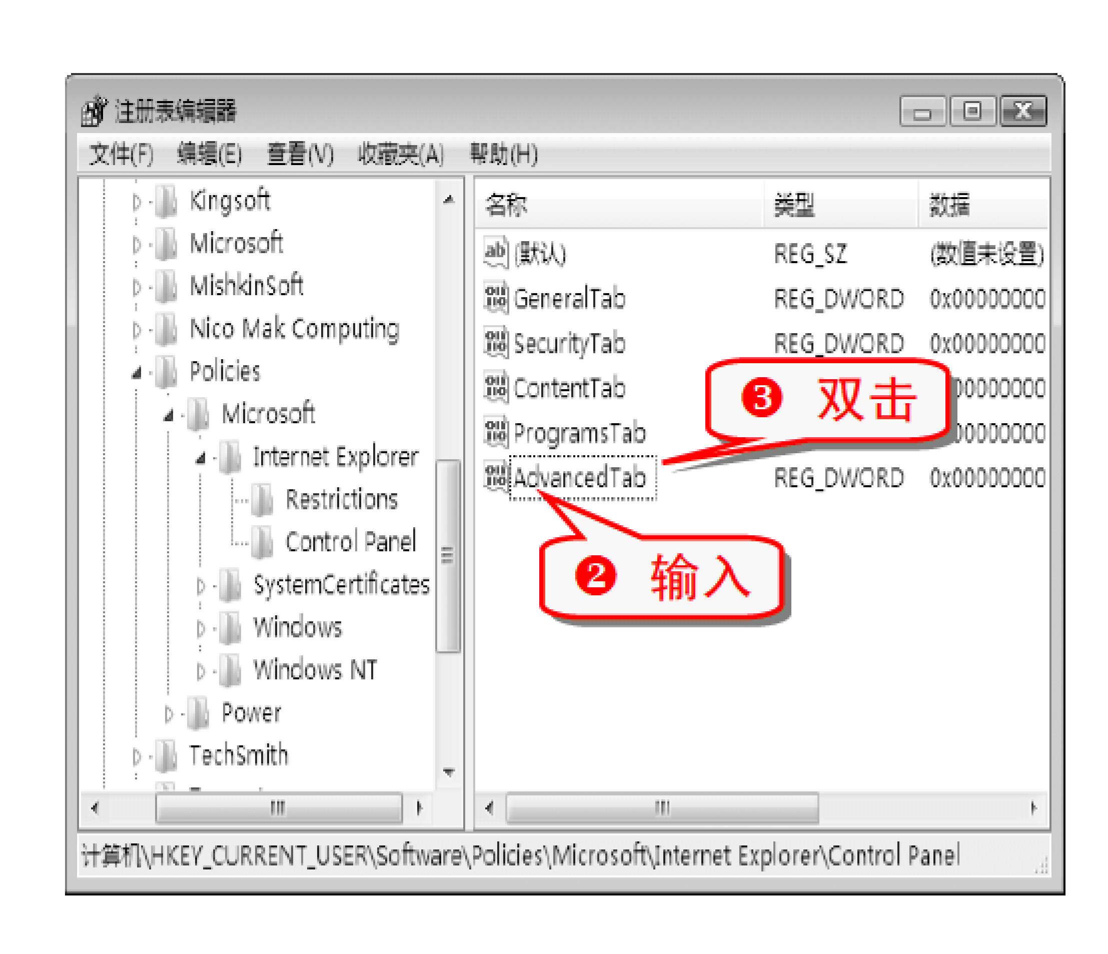
将 ProgramsTab 的键值设置为 0 即可让“程序”选项卡重新显示出来。设置在刷新后生效。

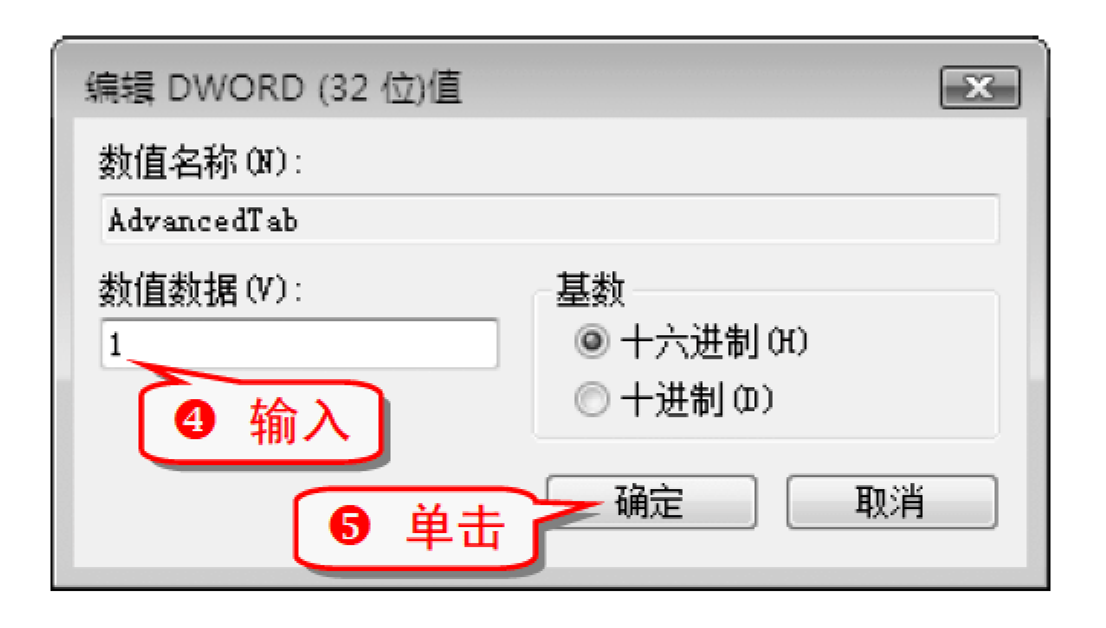
技巧165　禁用 Internet 选项的“高级”选项卡

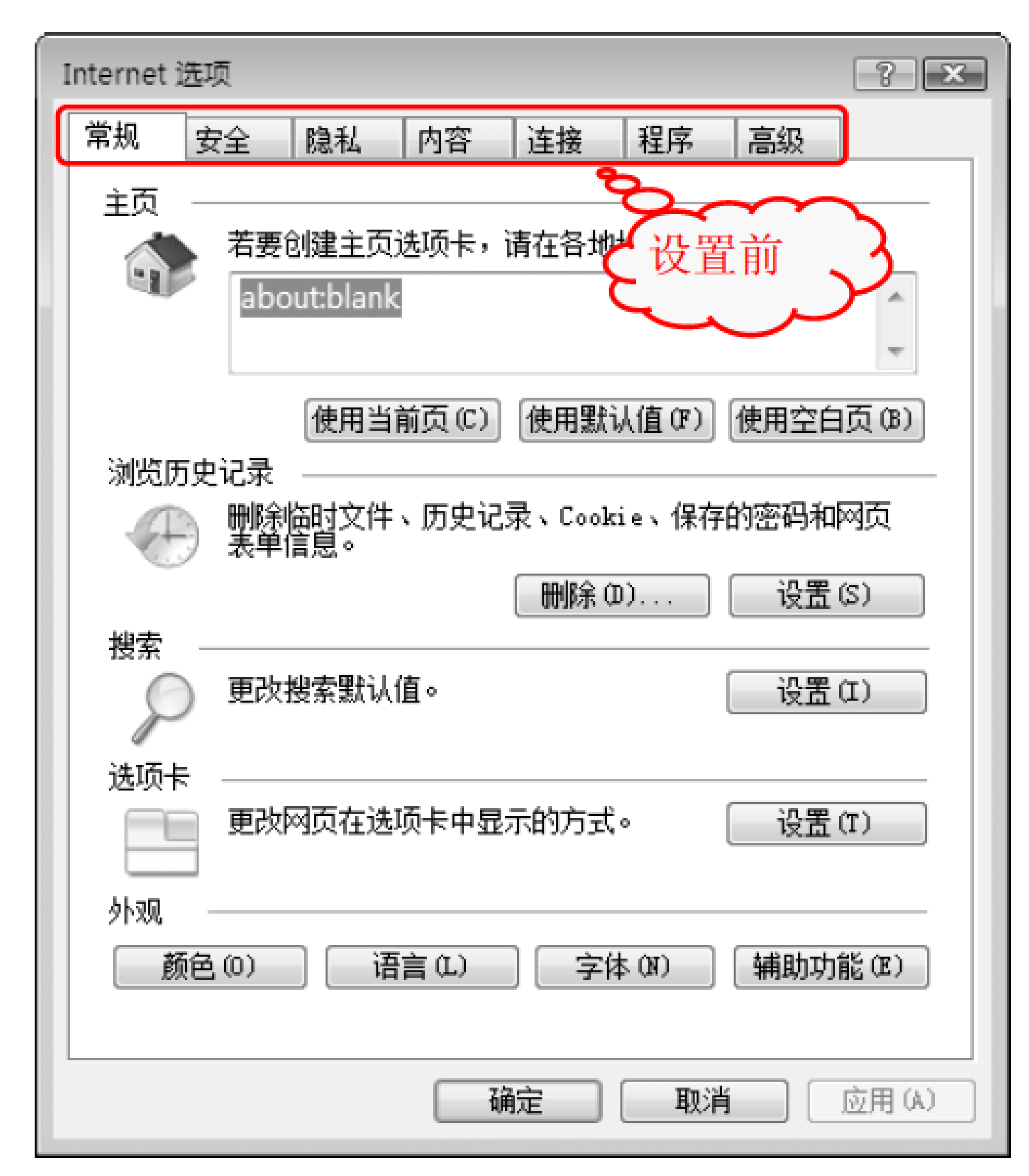
禁用 Internet 选项的“高级”选项卡，可以防止其他用户修改 HTTP、安全、打印、多媒体和辅助方向的设置。

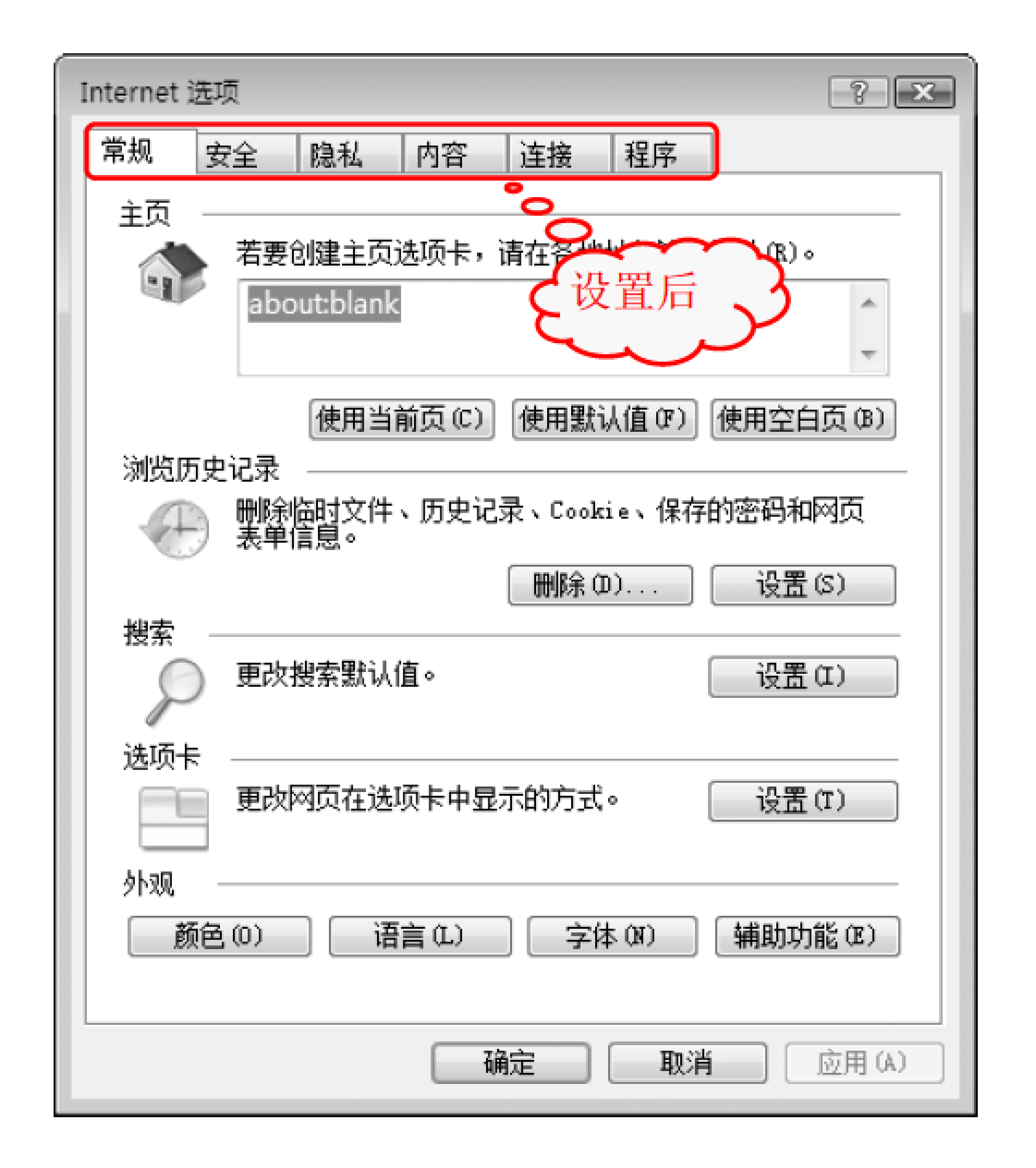
通过以下操作可以禁用 Internet 选项的“高级”选项卡。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel 分支，新建一个类型为 DWORD(32 位)的键值项。









注 意 事 项

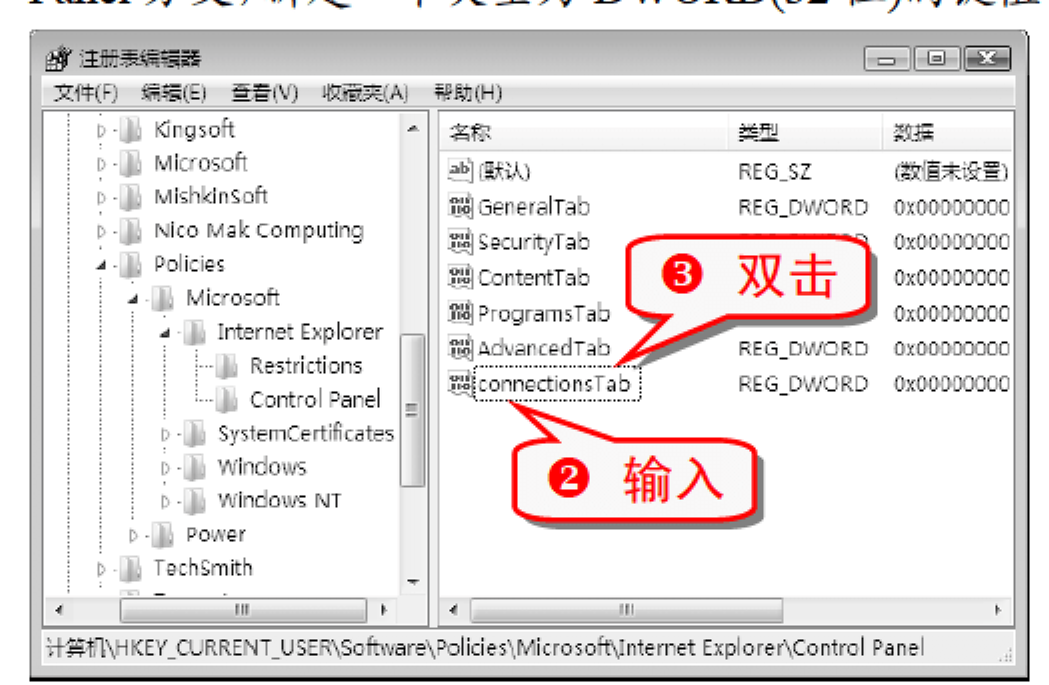
将 AdvancedTab 的键值设置为 0 即可让“高级”选项卡重新显示出来。设置在刷新后生效。

技巧166 禁用 Internet 选项的“连接”选项卡

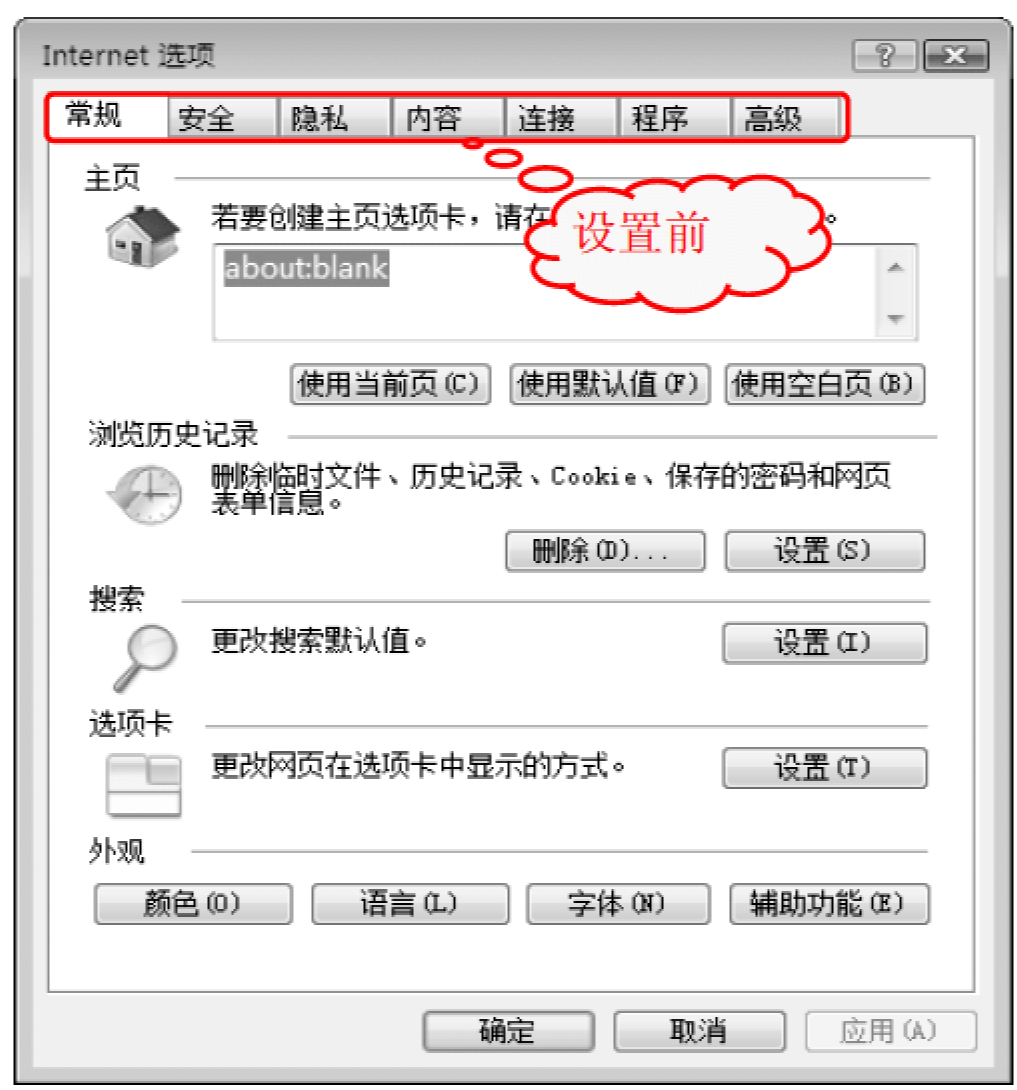
禁用 Internet 选项的“连接”选项卡，可以防止其他用户修改连接设置和局域网设置。

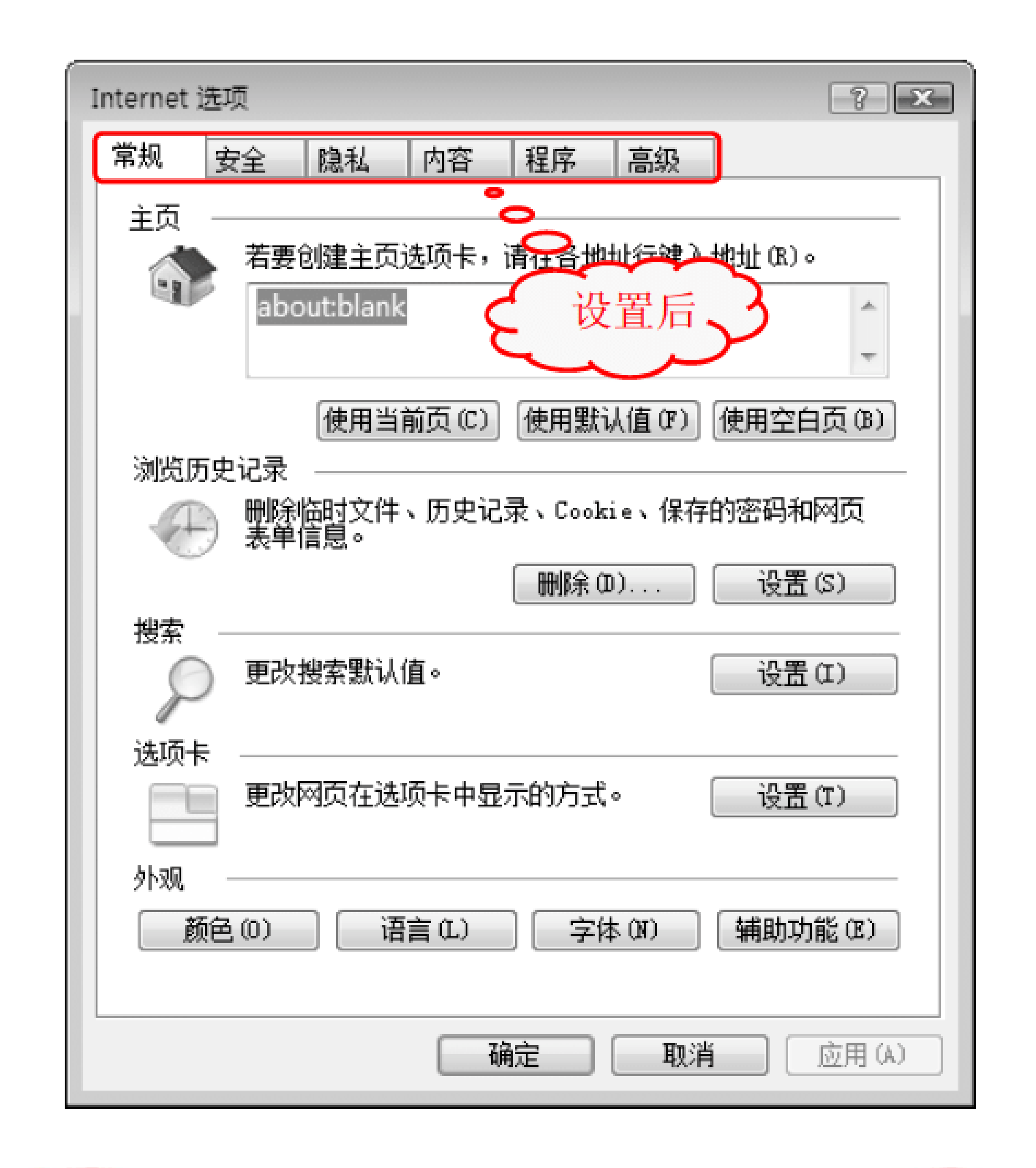
通过以下操作可以禁用 Internet 选项的“连接”选项卡。

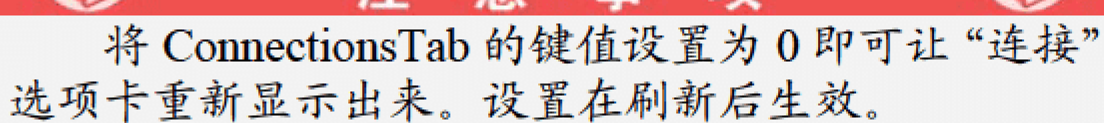
❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel 分支，新建一个类型为 DWORD(32 位)的键值项。











注 意 事 项

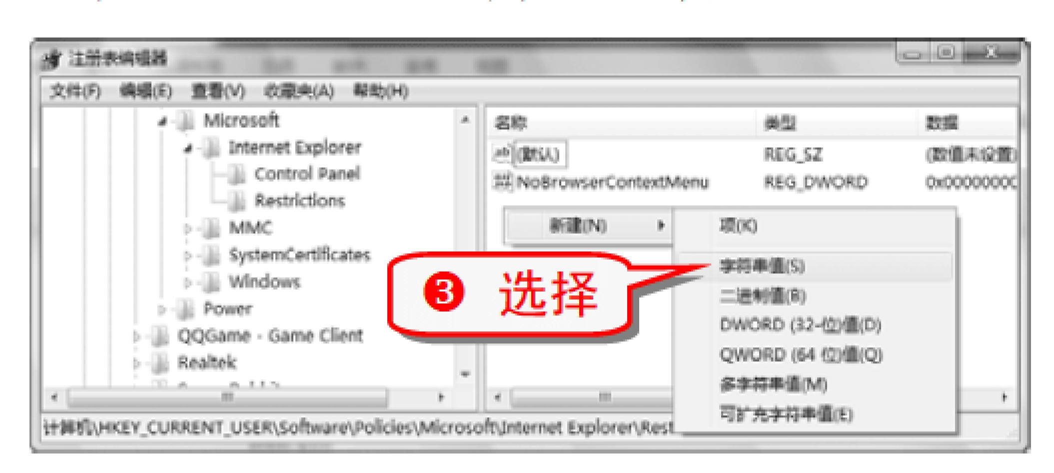
将 ConnectionsTab 的键值设置为 0 即可让“连接”选项卡重新显示出来。设置在刷新后生效。

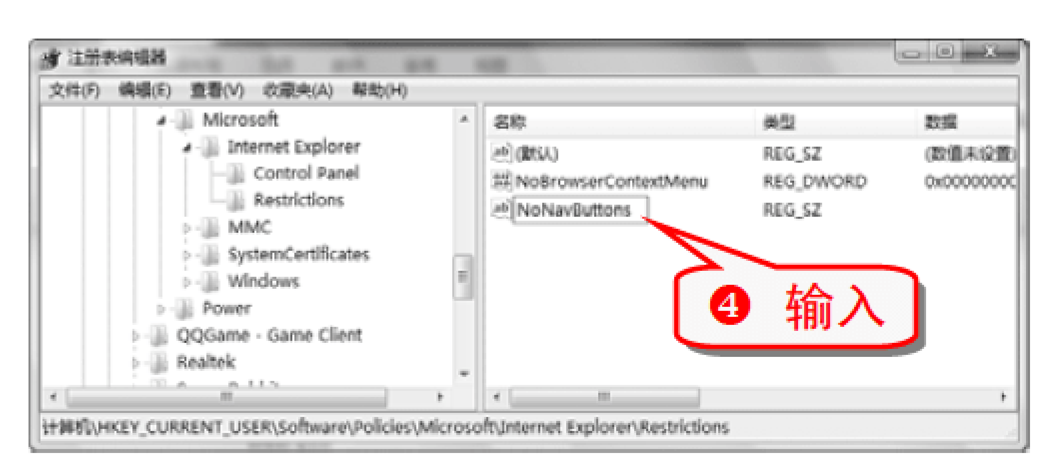
技巧167 禁用 IE 导航“后退”和“前进”按钮

禁用 IE 导航“后退”和“前进”按钮，避免浏览器随意弹出网页。

❶ 打开注册表编辑器，展开 HKEY_CURR ENT_USER\Software\Policies\Microsoft\InternetExplorer\Restrictions 分支。

❷ 选择 Restrictions 选项并在右边窗格空白处右击。





❺ 选中 NoNavButtons 选项并双击。



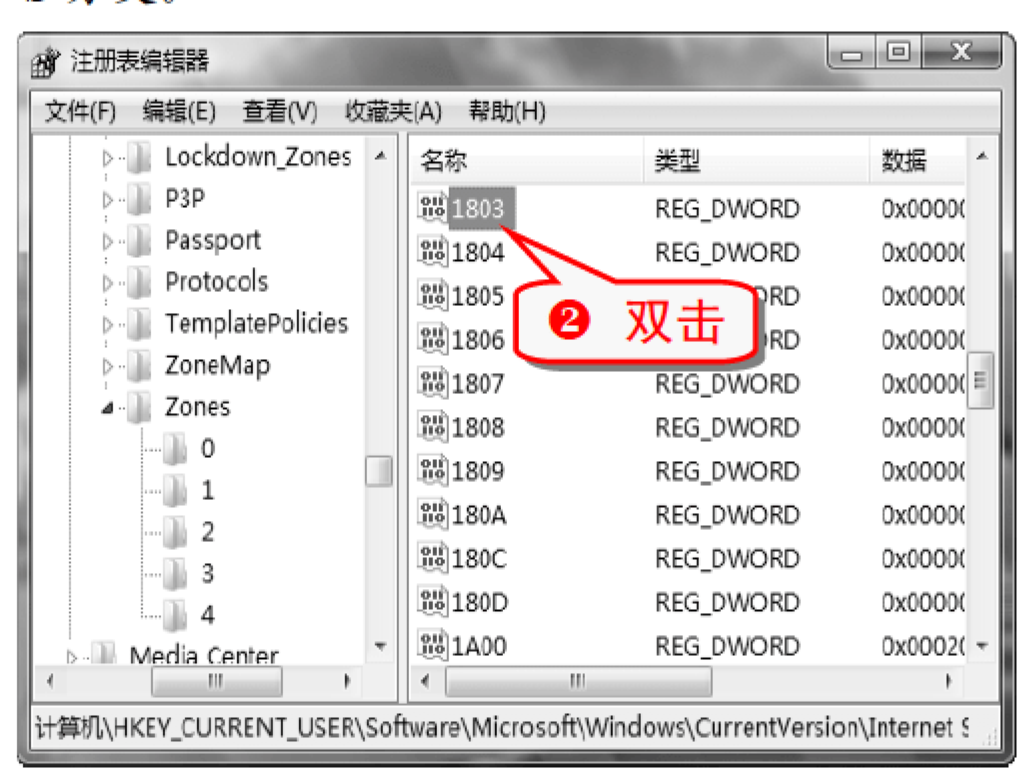


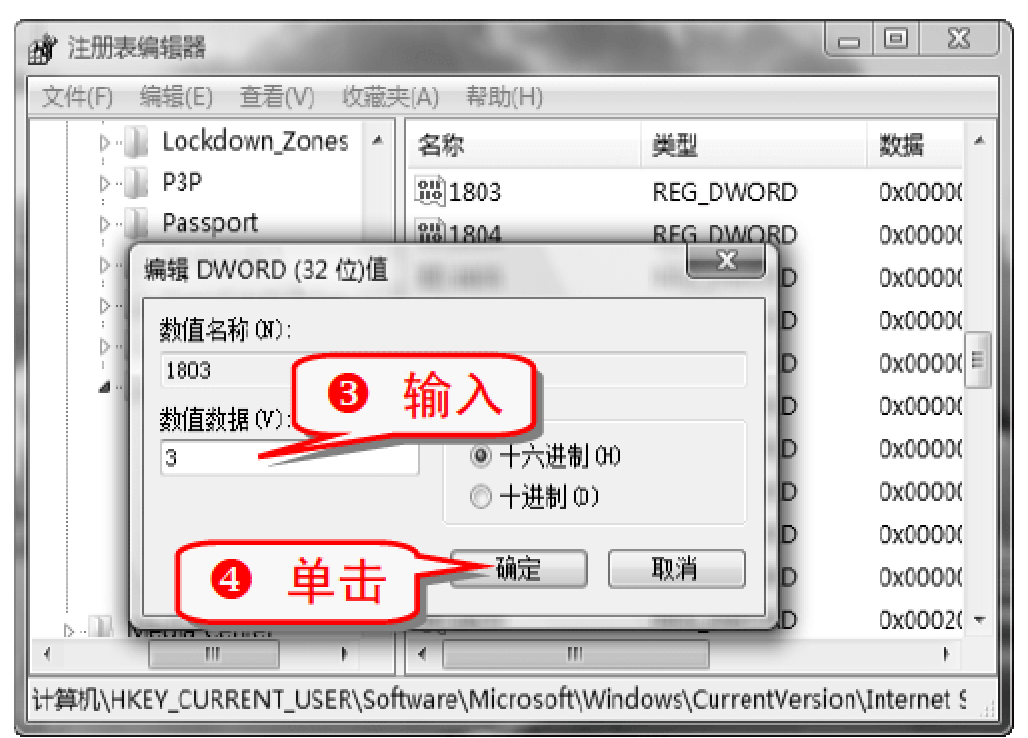
技巧168　禁止通过 IE 下载

在局域网中下载文件会影响网速，而且从网上下载的文件很容易带有病毒，如果不希望用户通过网页下载文件，可以将 IE 的下载功能禁止。

(1) 通过修改注册表禁止 IE 下载

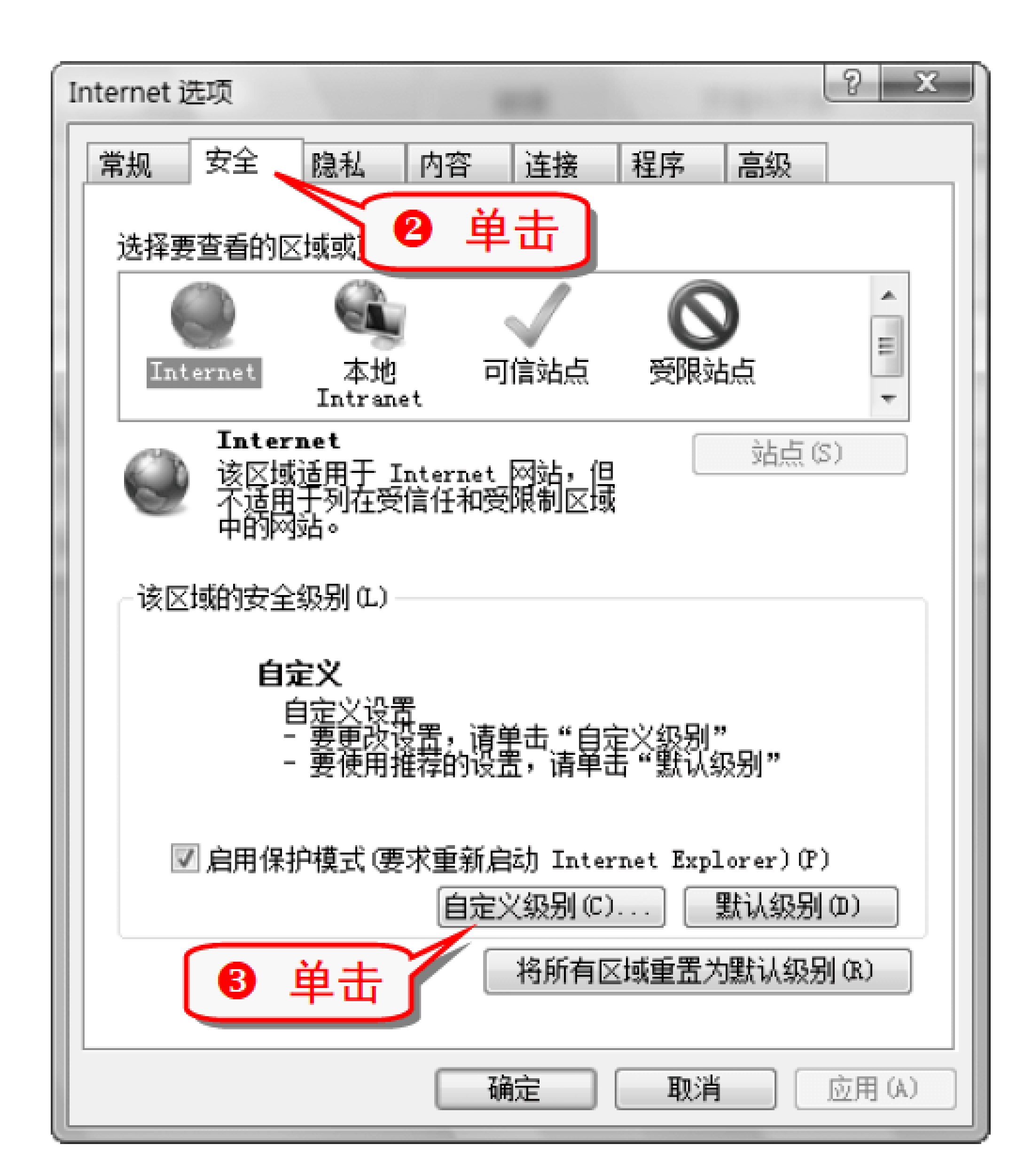
❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Windows\CurrentVersion\Interner Setting\Zones\3 分支。

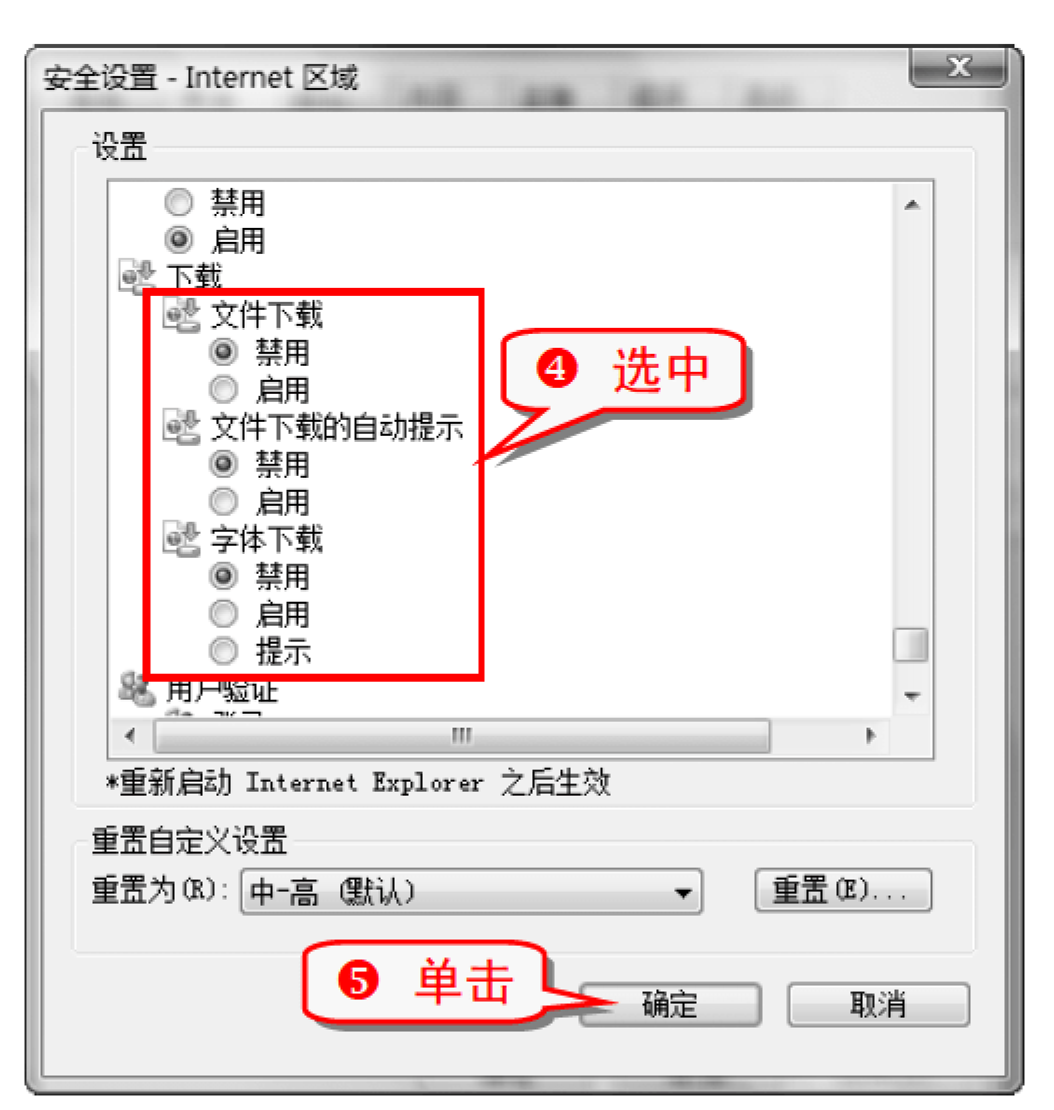




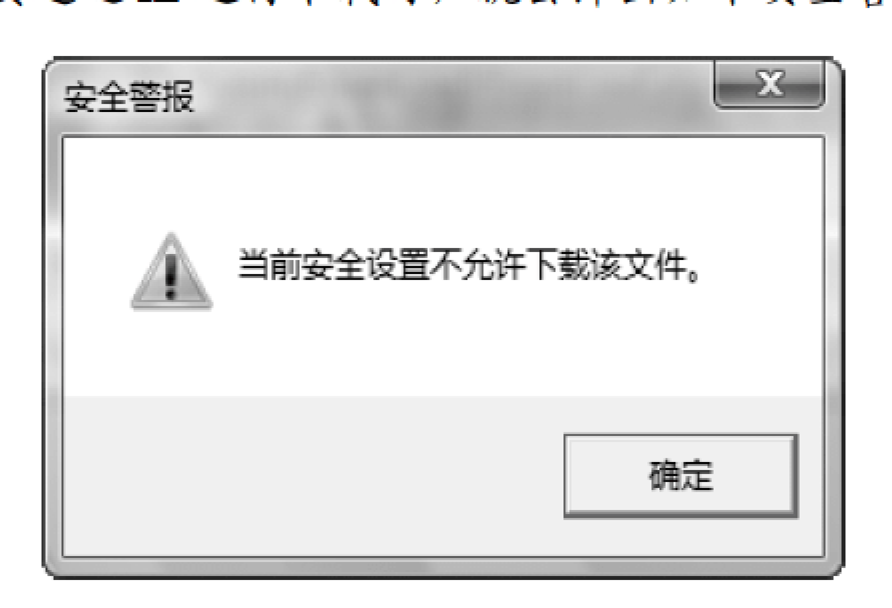
(2) 通过设置 IE 选项禁止 IE 下载

❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框。





❻ 当要通过 IE 进行下载时，就会弹出如下安全警报框。



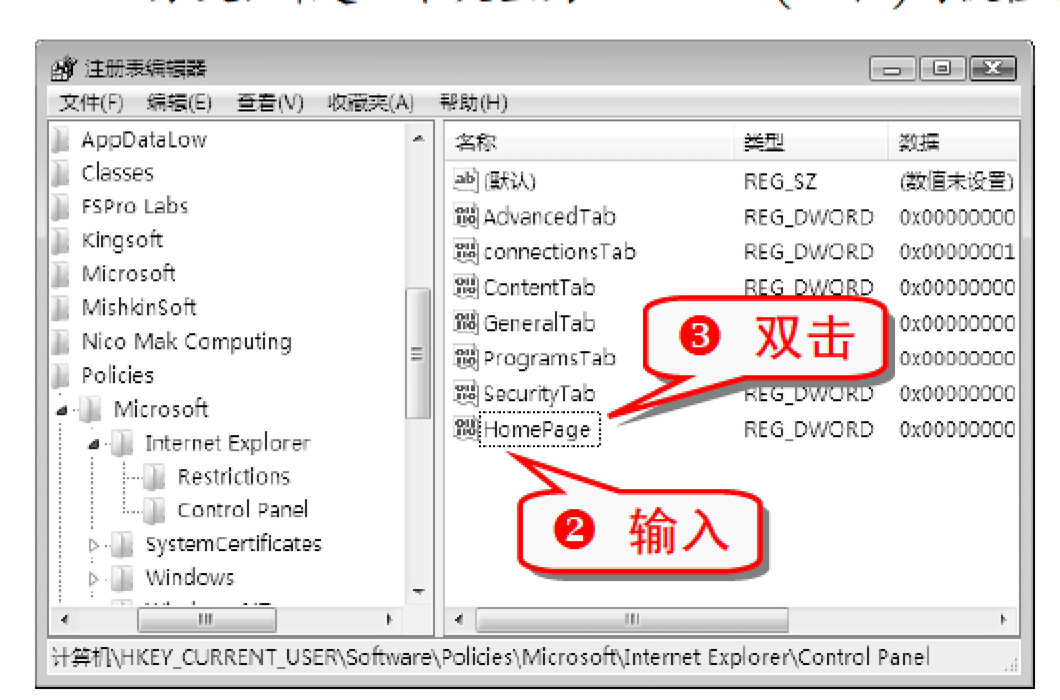
技巧169　禁止更改 IE 浏览器的主页

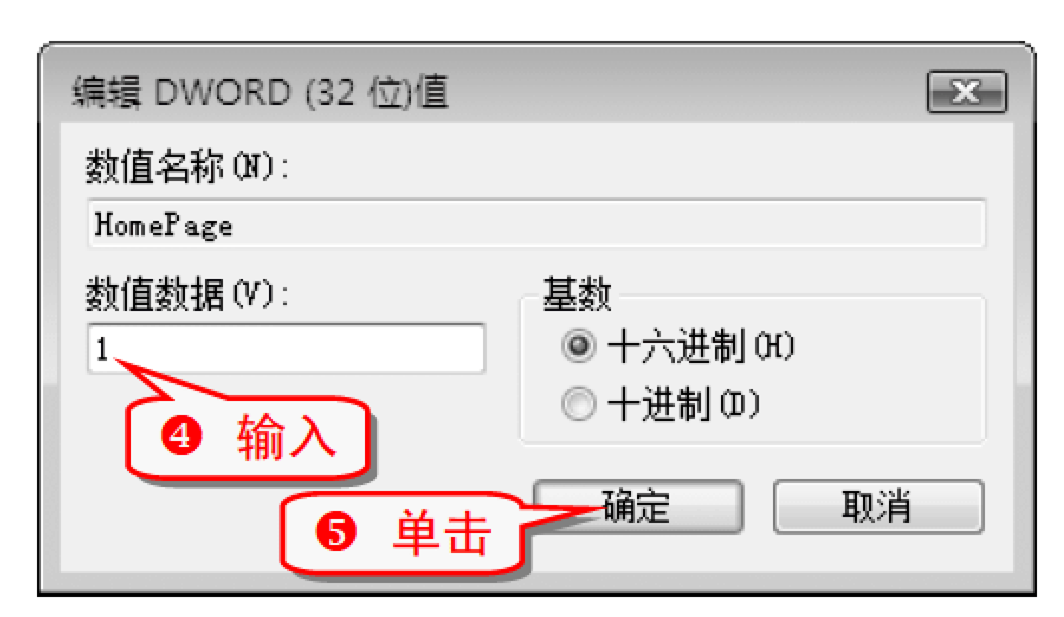
在上网过程中，由于安装了某些插件或者中了木马，

IE 浏览器的主页会被恶意更改，打开 IE 浏览器后会链接进入特定的网站。

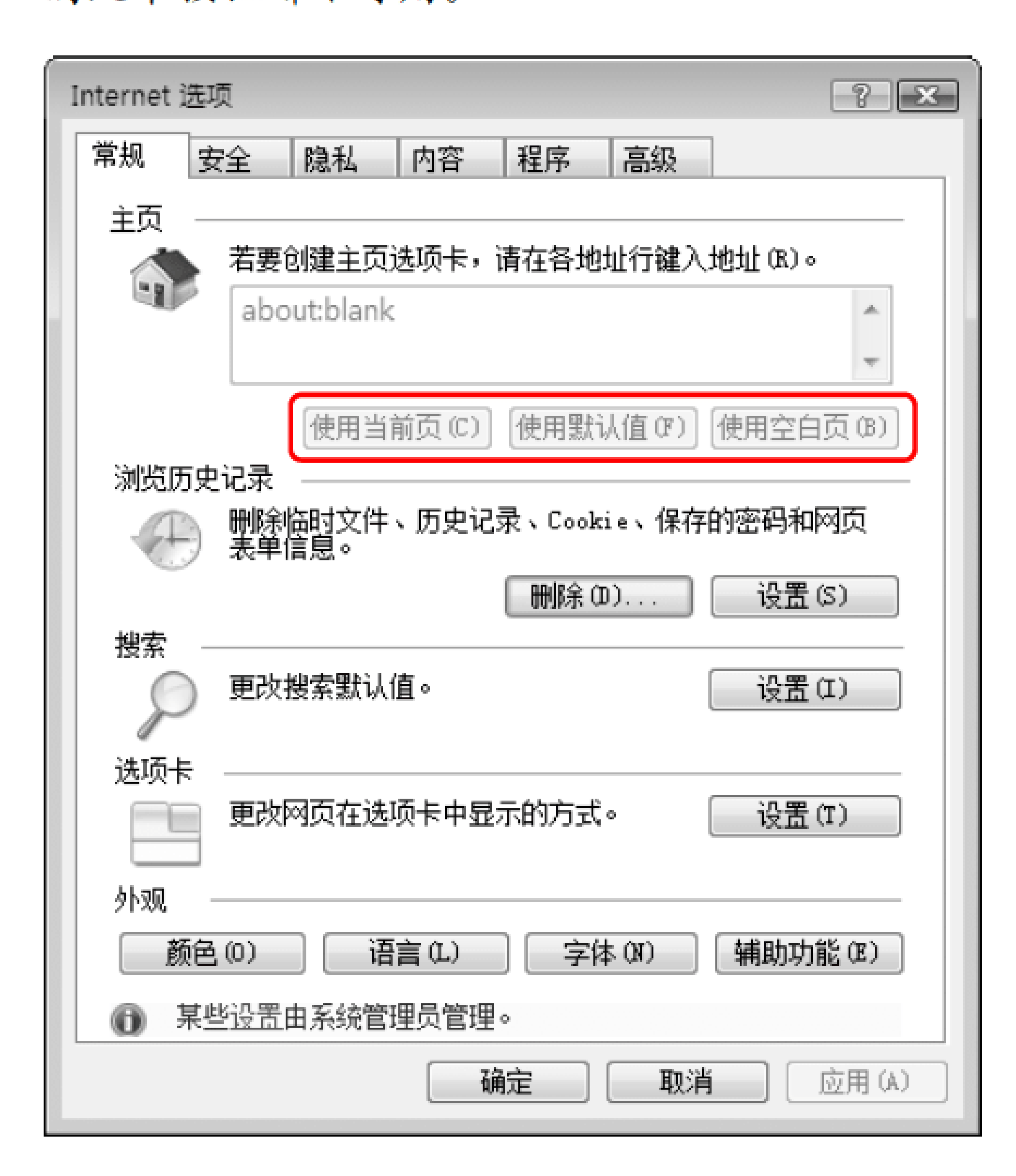
通过以下操作可以防止恶意代码更改 IE 浏览器的主页。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel 分支，新建一个类型为 DWORD(32 位)的键值项。





❻ 刷新后打开"Internet 选项"对话框可以发现设置主页的几个按钮都不可用。



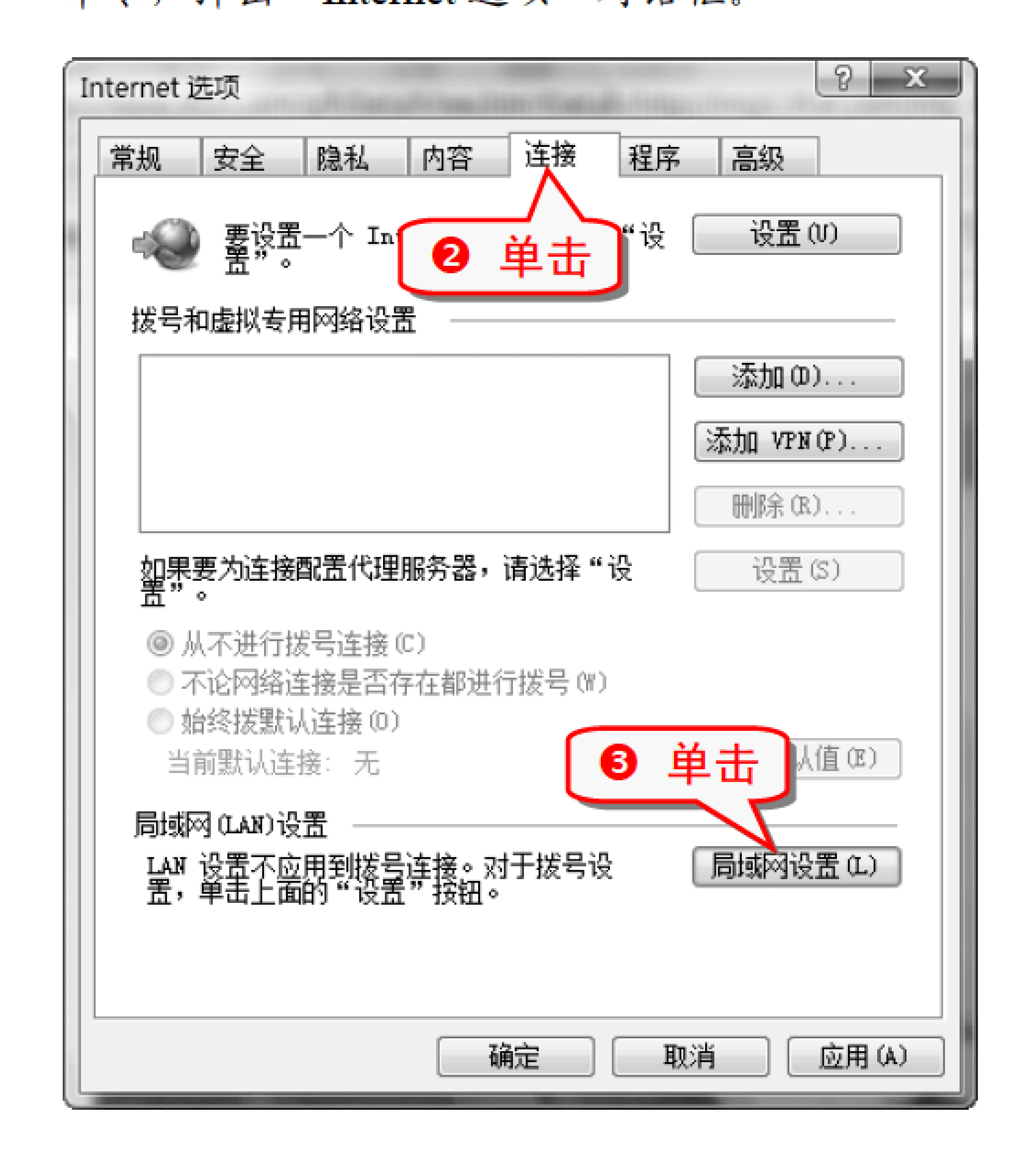

注 意 事 项

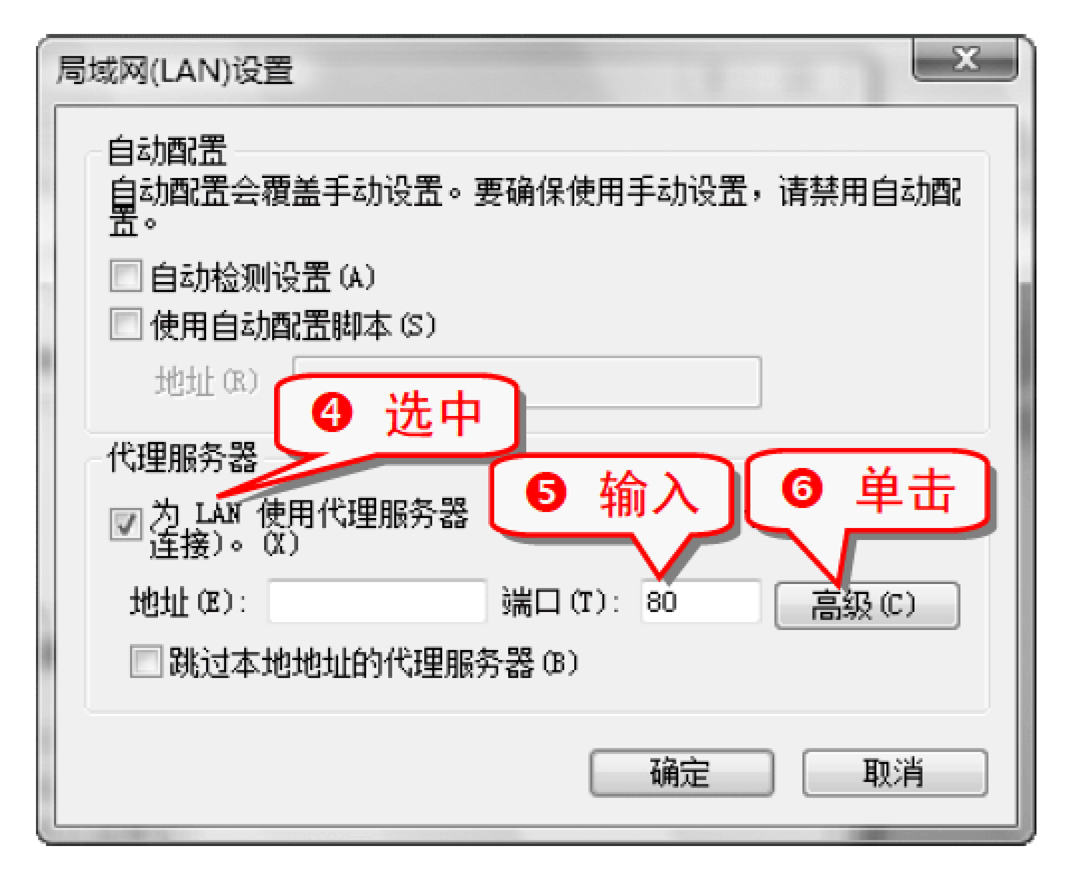
将 HomePage 的键值设置为 0 即可重新启用 IE 的主页设置功能。设置在刷新后生效。

技巧170 巧用代理服务器保护 IE 上网安全

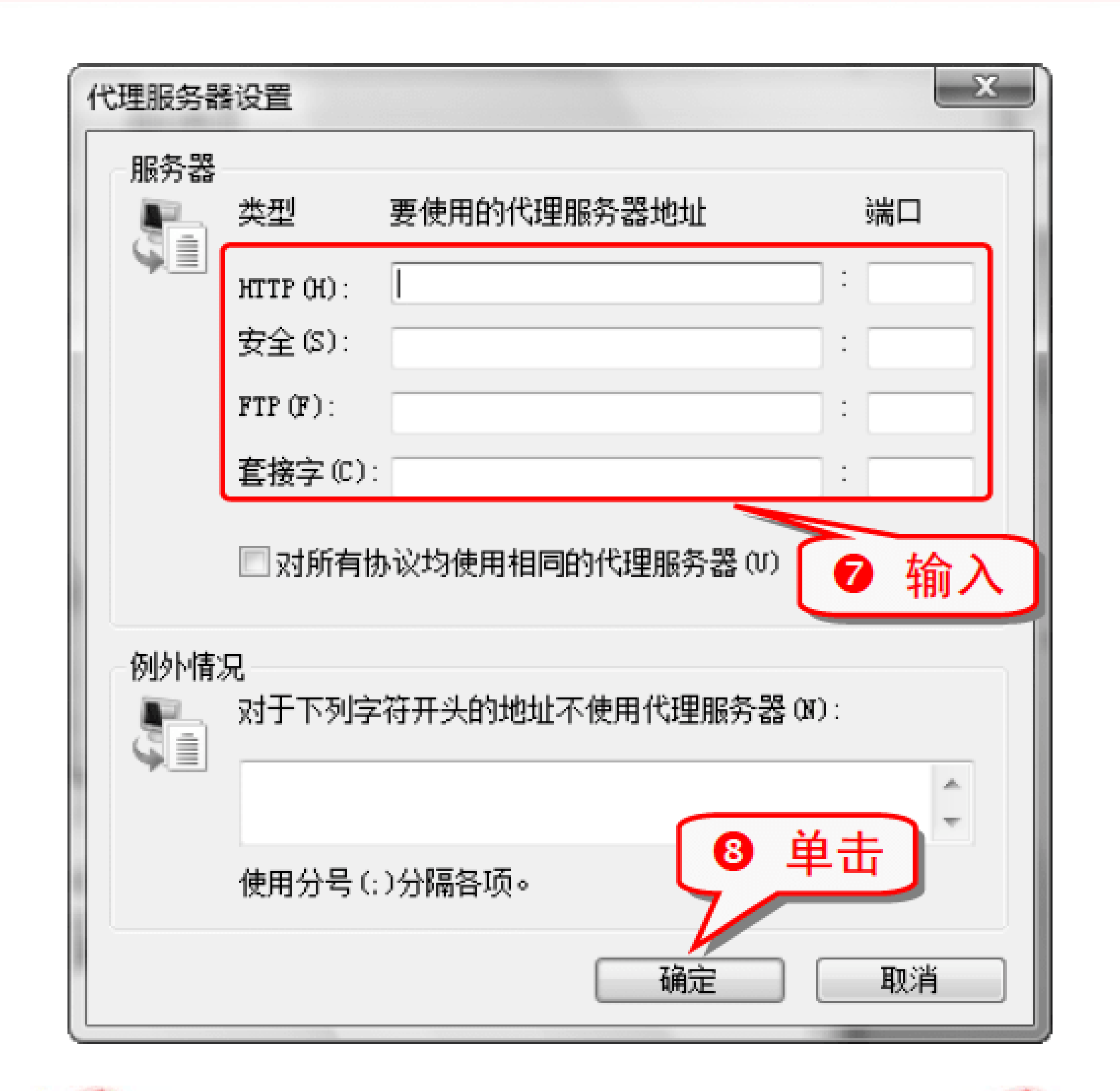
代理服务器是在 Web 浏览器和 Internet 之间起媒介作用的计算机。代理服务器通过存储经常使用的网页副本来提高 Web 浏览器的性能。用户使用代理服务器时，还可以过滤一些恶意软件，从而提高上网的安全性。

❶ 在打开的 IE 浏览器中选择"工具"→"Internet 选项"命令，弹出"Internet 选项"对话框。









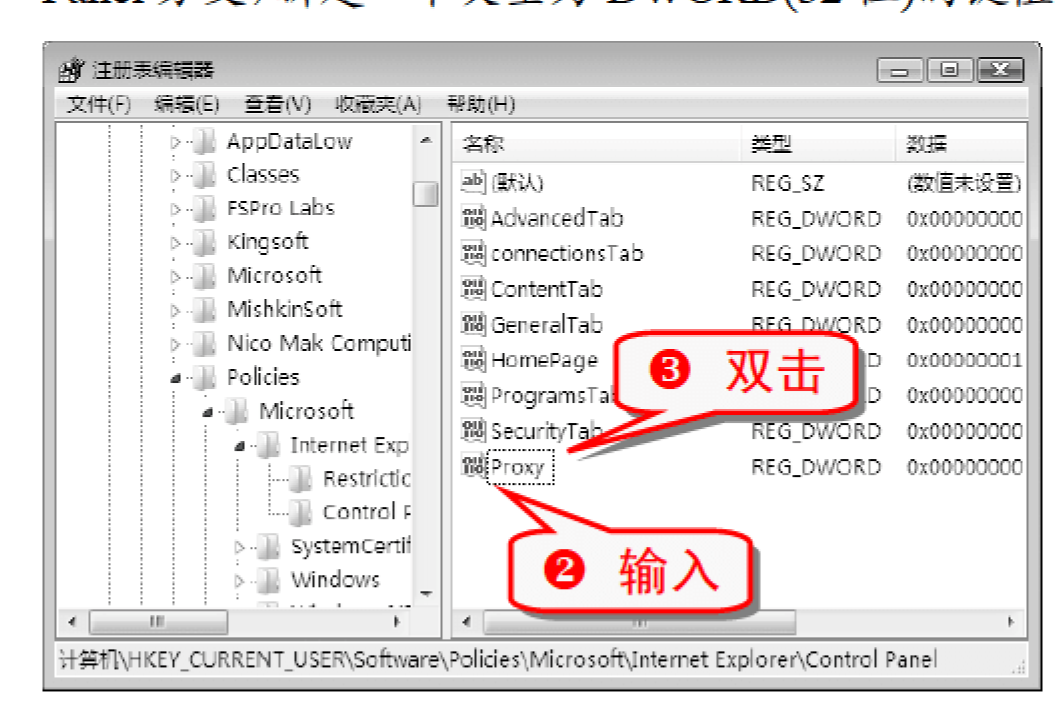
专 家 坐 堂

代理服务器多数在组织和公司中的网络使用，家庭中的计算机连接到 Internet 不需要使用代理服务器。在默认情况下，IE 将会自动检测代理设置，但是可能也需要网络管理员提供的信息来手动完成设置。

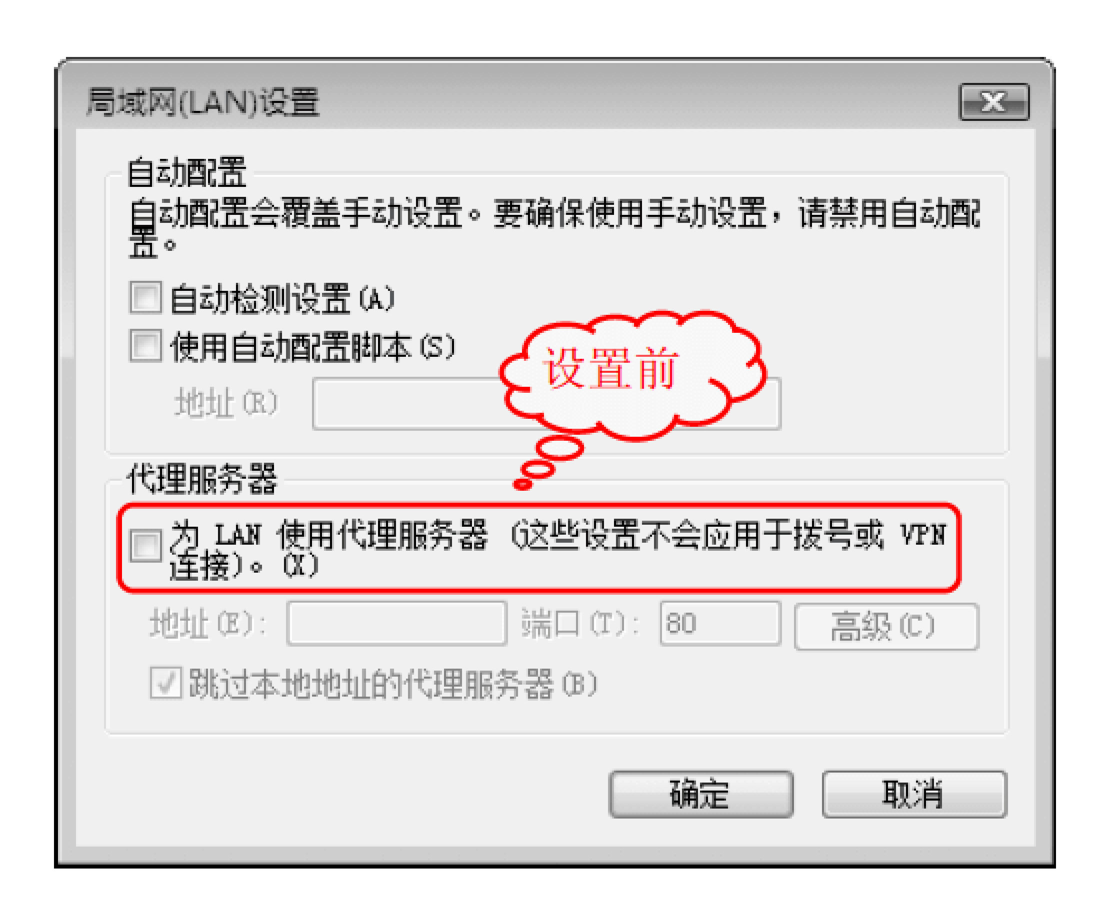
技巧171 禁止更改 IE 代理服务器

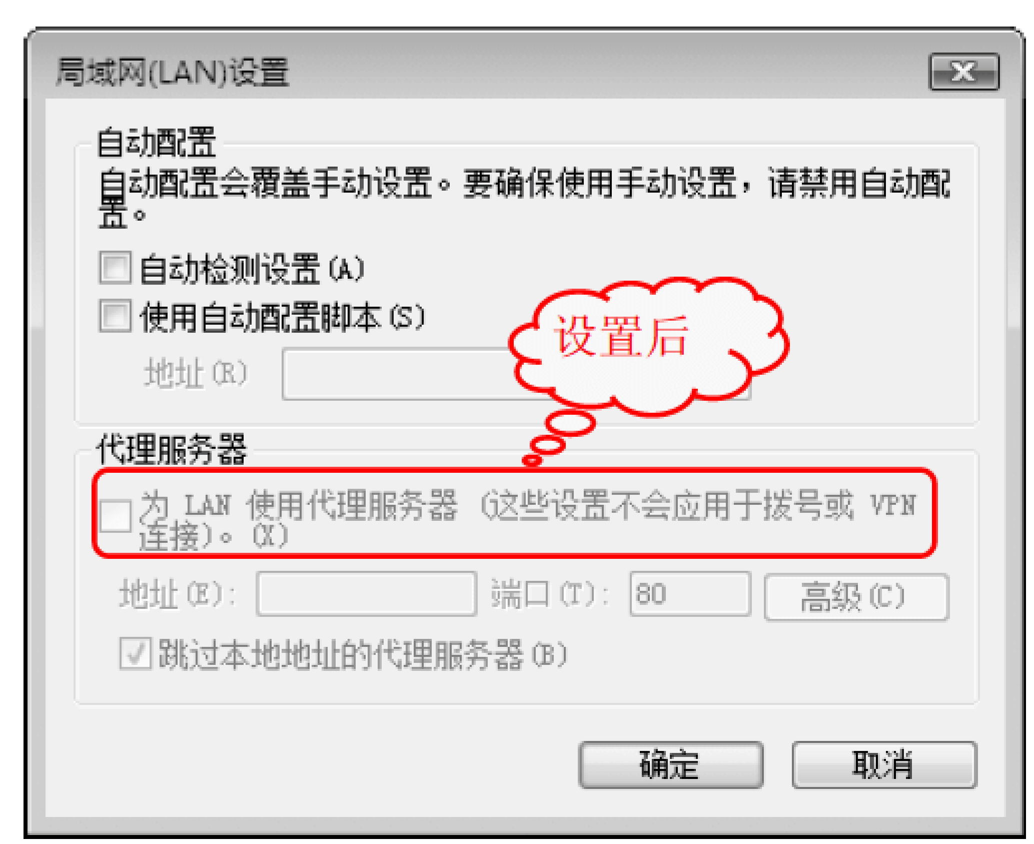
通过以下操作可以防止更改已经设置好的 IE 代理服务器。

❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel 分支，新建一个类型为 DWORD(32 位)的键值项。









注 意 事 项

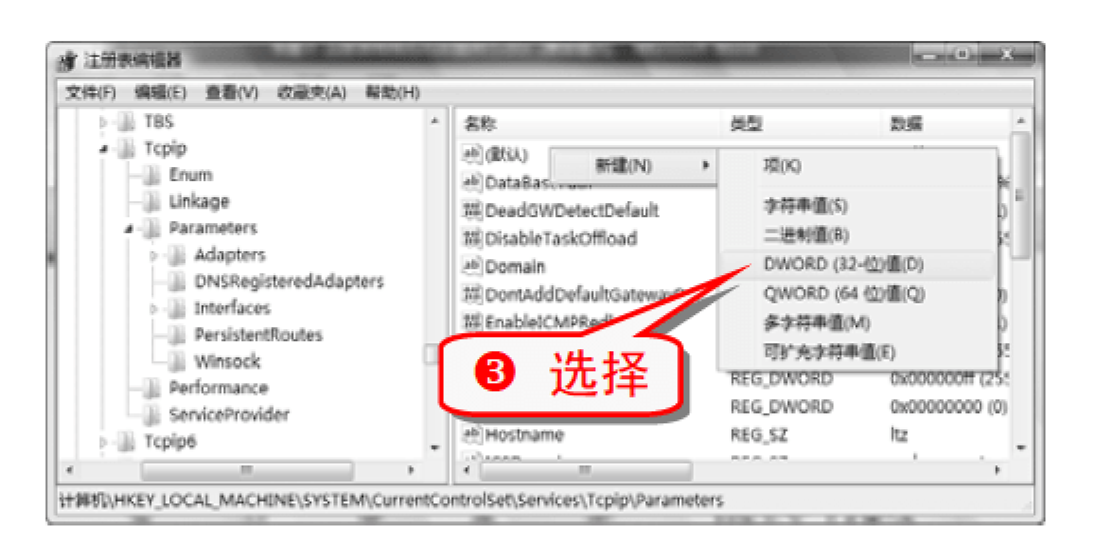
将 Proxy 的键值设置为 0 即可重新启用设置代理服务器的功能。设置在刷新后生效。

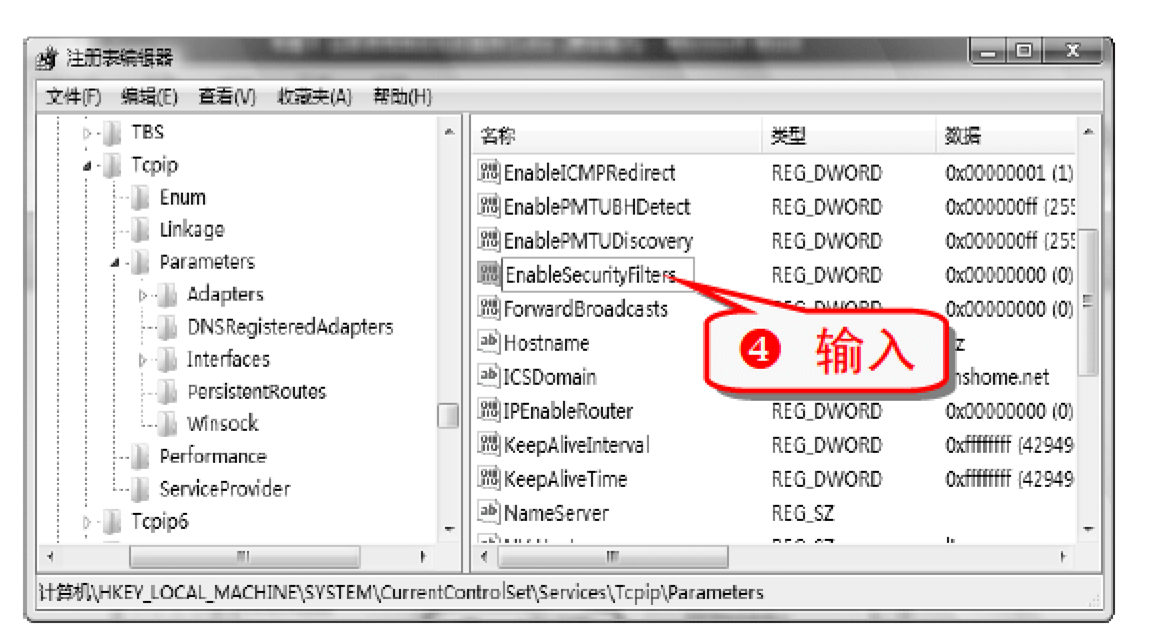
技巧172 过滤 IP 地址

过滤 IP 地址可以过滤带有恶意插件或病毒的网页，提高 IE 的防御力。

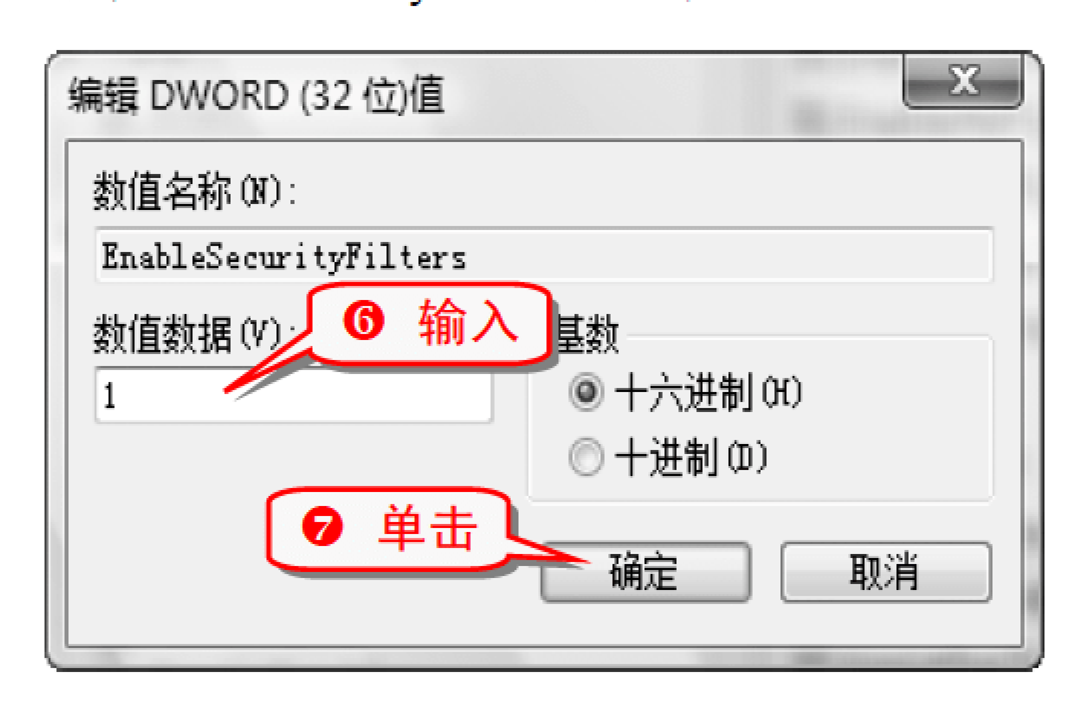
❶ 打开注册表编辑器，展开 HKEY_LOCA L_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 分支。

❷ 选择 Parameters 选项并在右边窗格的空白处右击。





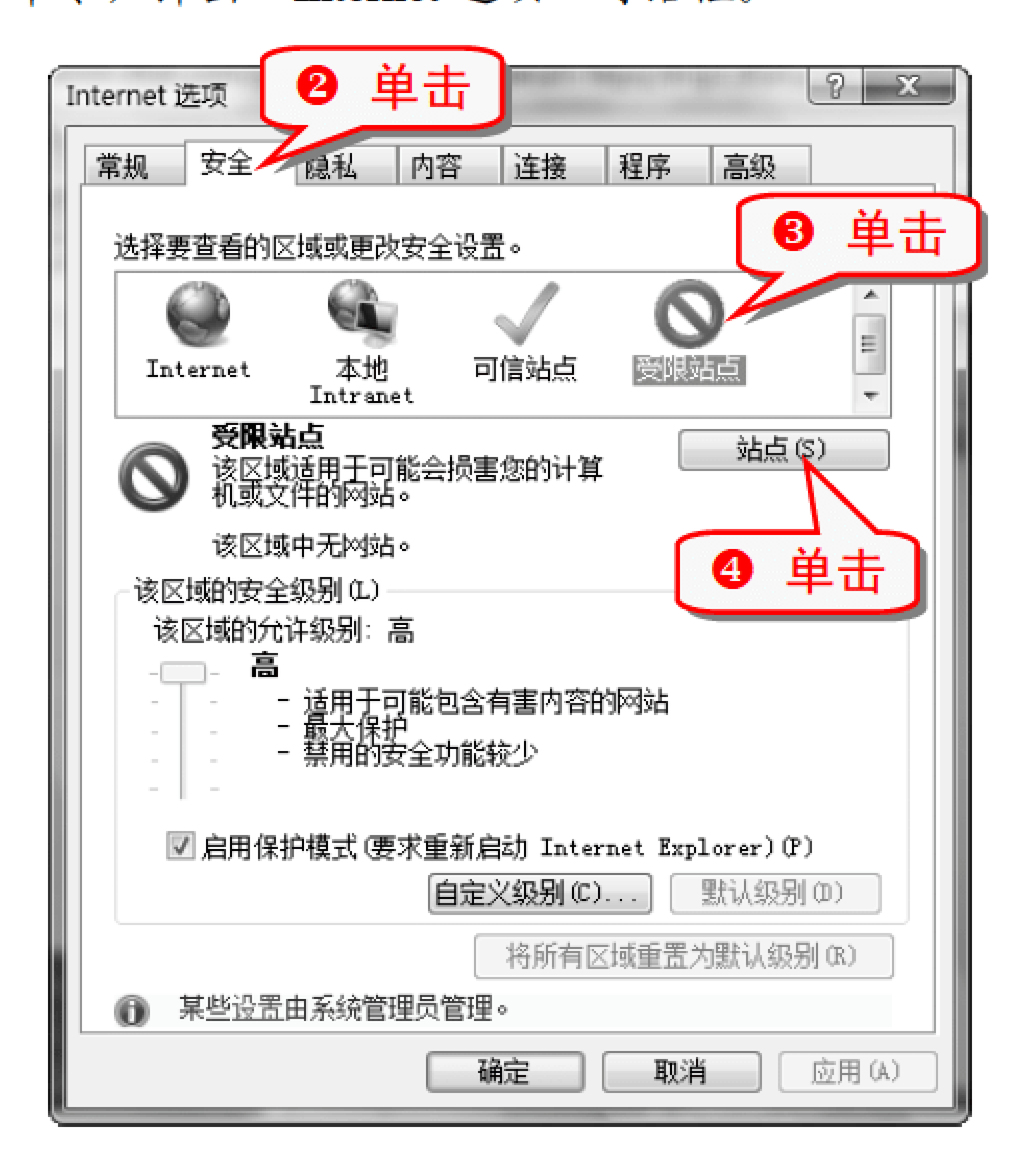
❺ 选择 EnableSecurityFilters 选项并双击。

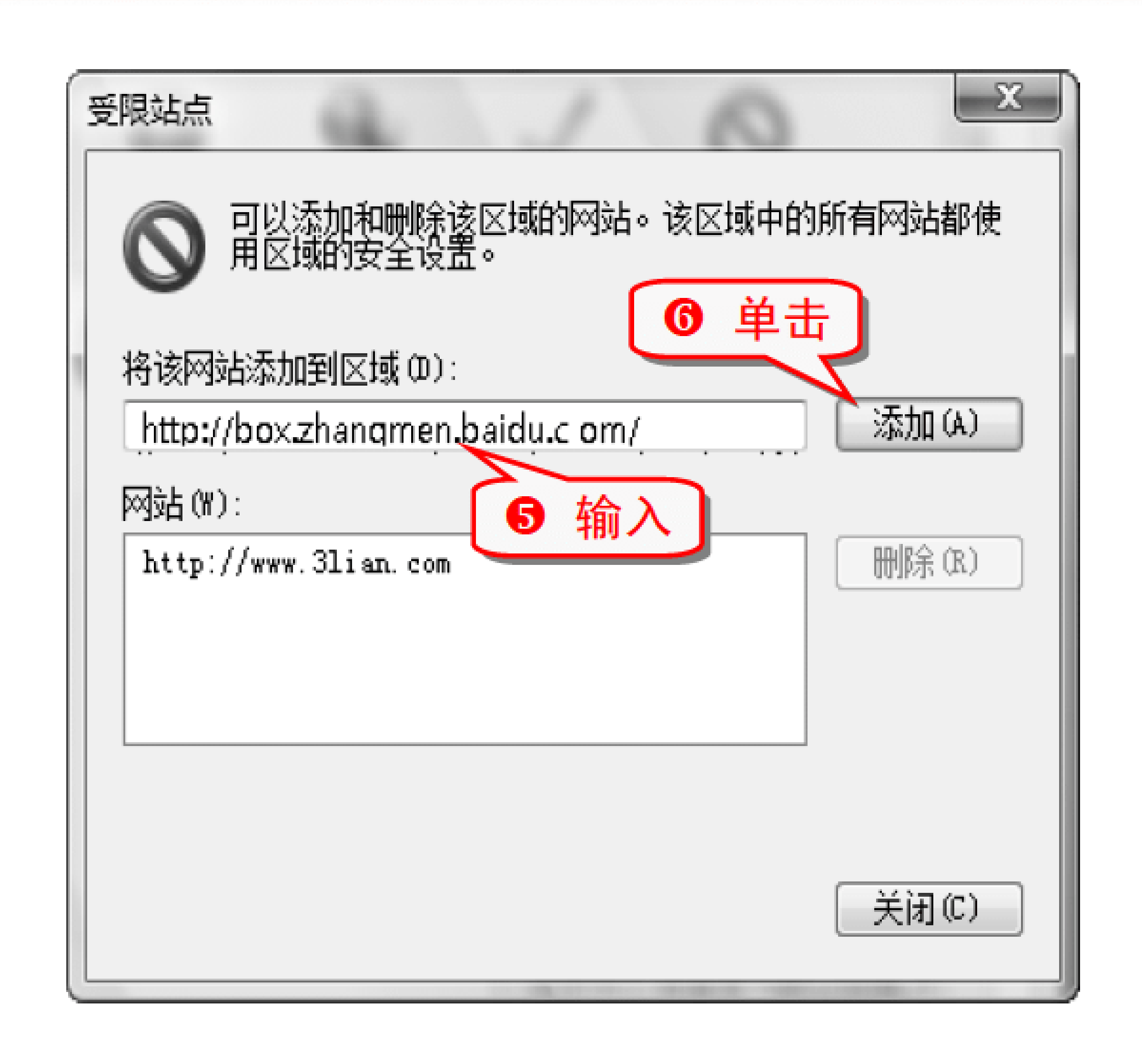


技巧173　巧用 IE 黑名单保护上网安全

浏览网页时，有时会弹出很多广告，不仅影响网页浏览，还会消耗大量的系统资源。根据系统自带的“受限站点”功能可以禁止这些广告弹出。

❶ 在打开的 IE 浏览器中选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框。

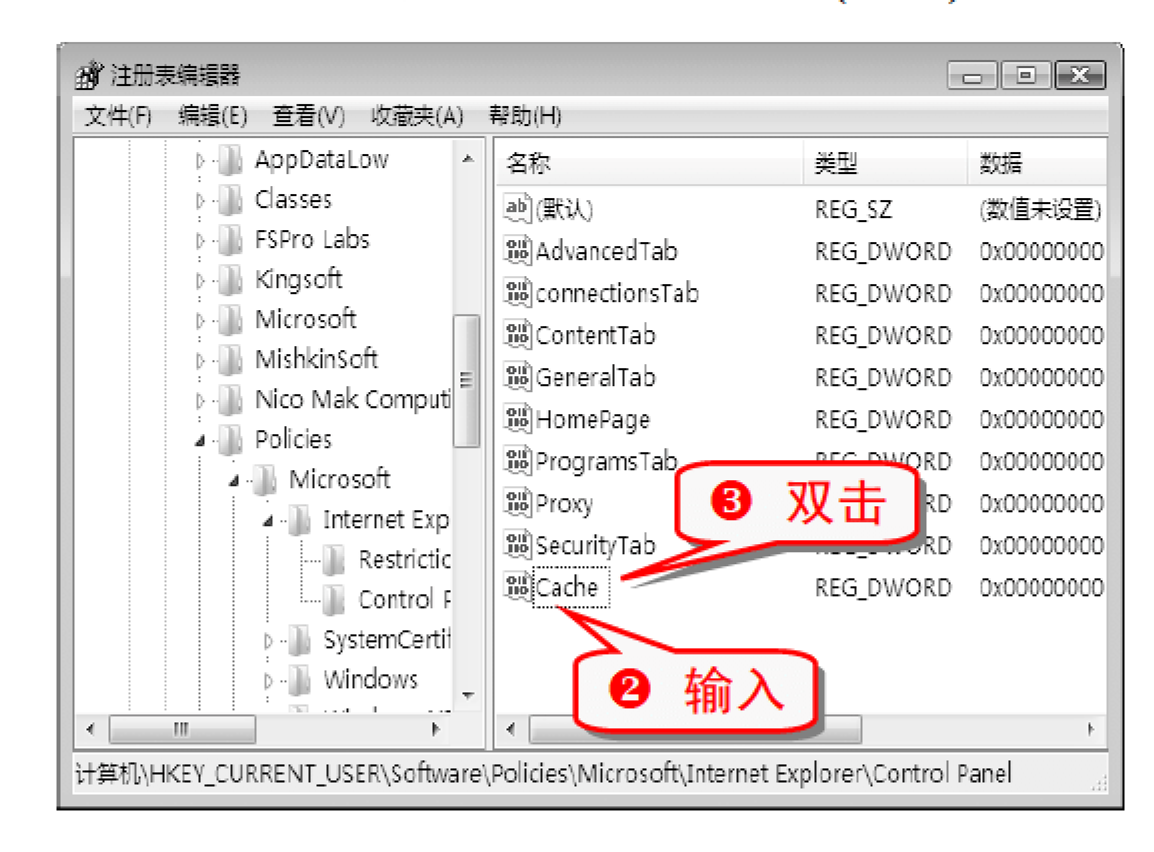


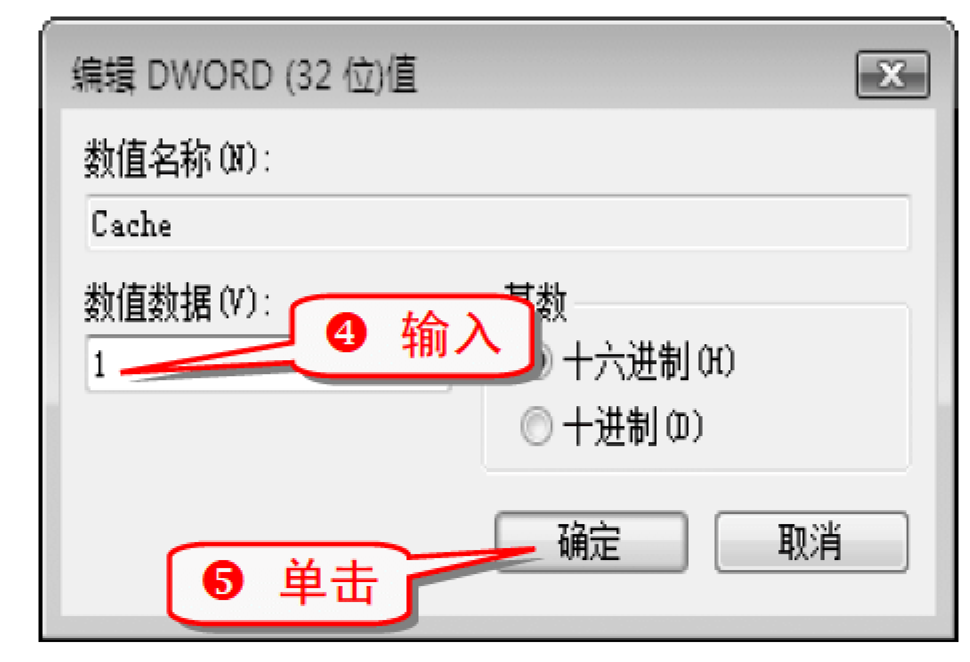


技巧174　禁止更改临时文件的设置

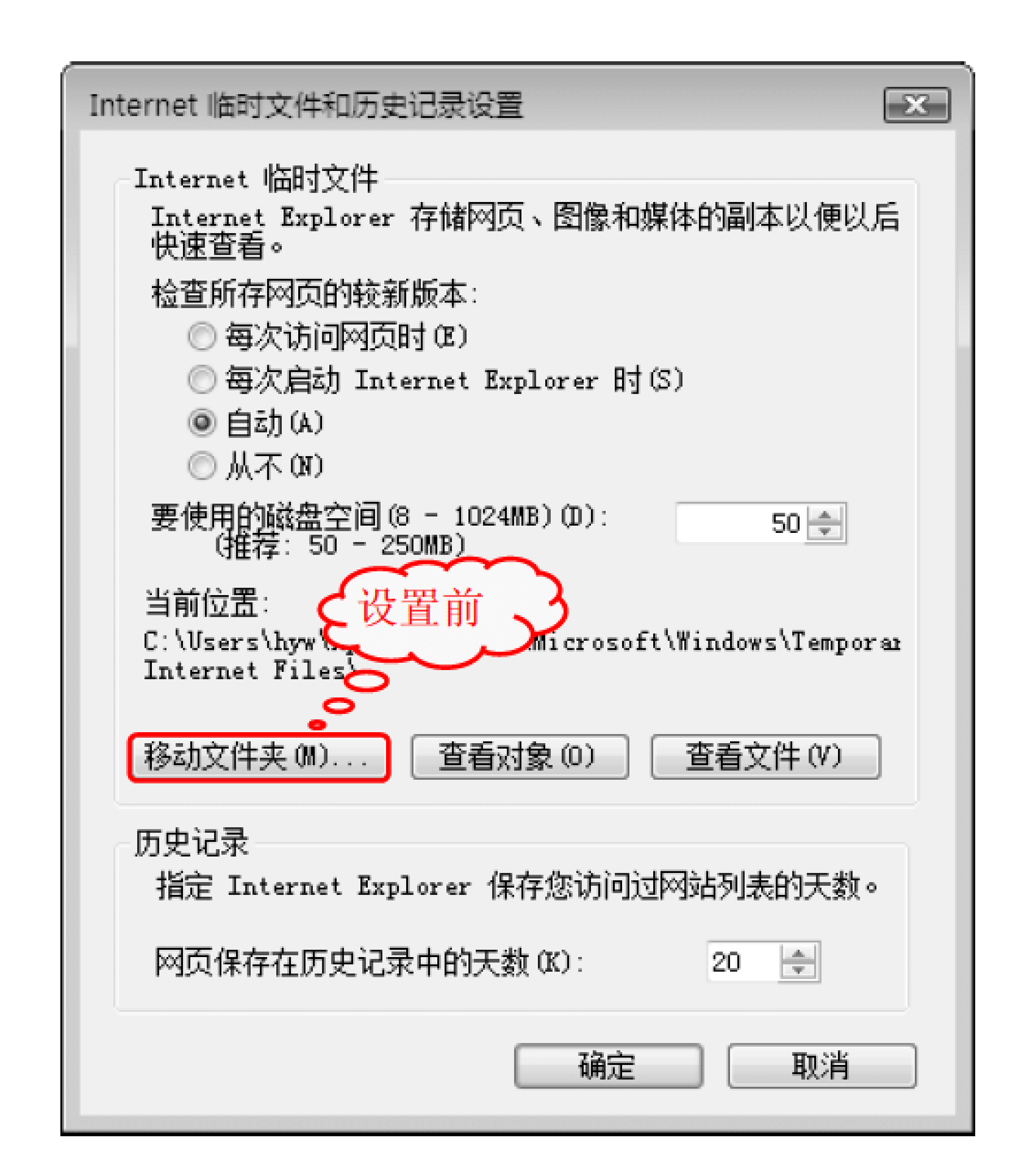
通过以下操作可以禁止更改临时文件的设置。

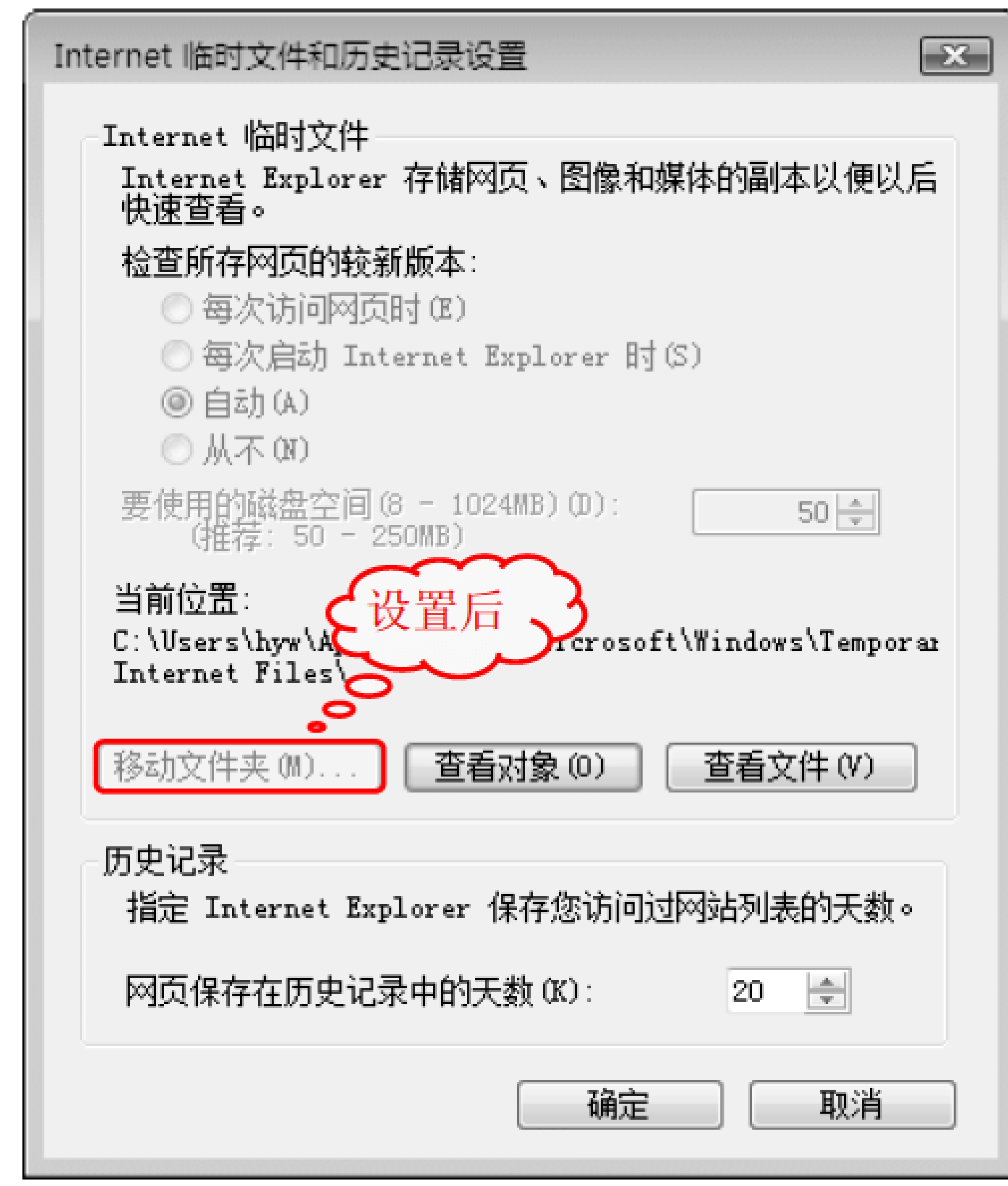
❶ 打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel 分支，新建一个类型为 DWORD(32 位)的键值项。

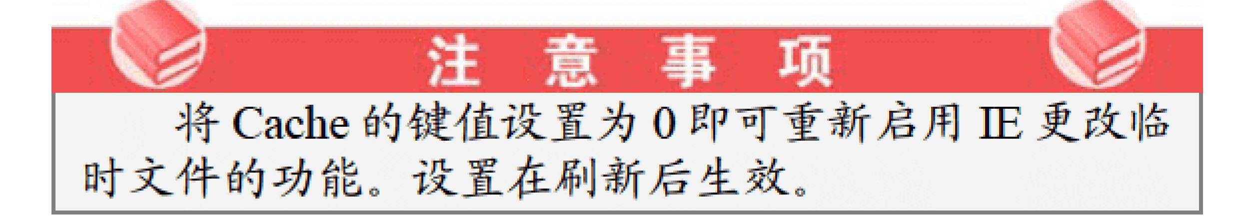










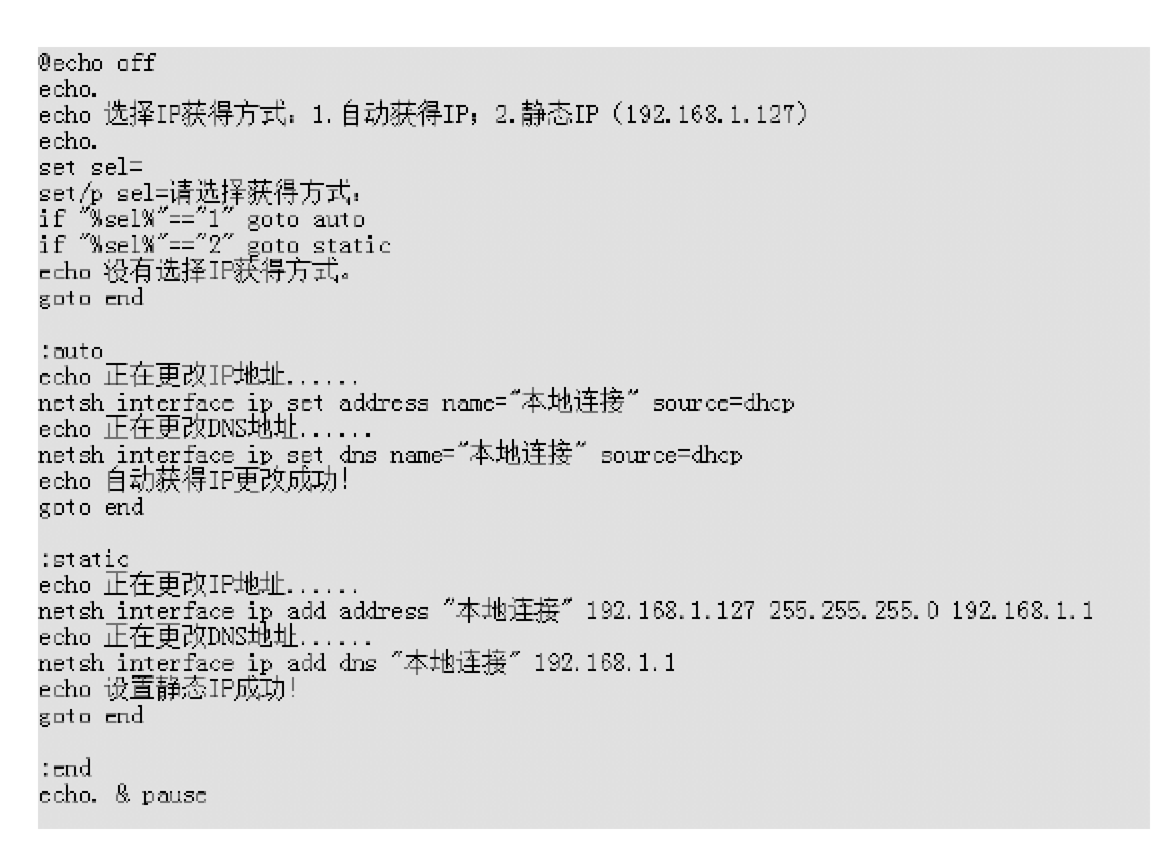


将 Cache 的键值设置为 0 即可重新启用 IE 更改临时文件的功能。设置在刷新后生效。

技巧175　巧用批处理命令更改 IP 地址

通过编写批处理命令的代码，可以快速更改当前计算机的 IP 地址。

❶ 新建一个文本文档，输入下面这段代码。



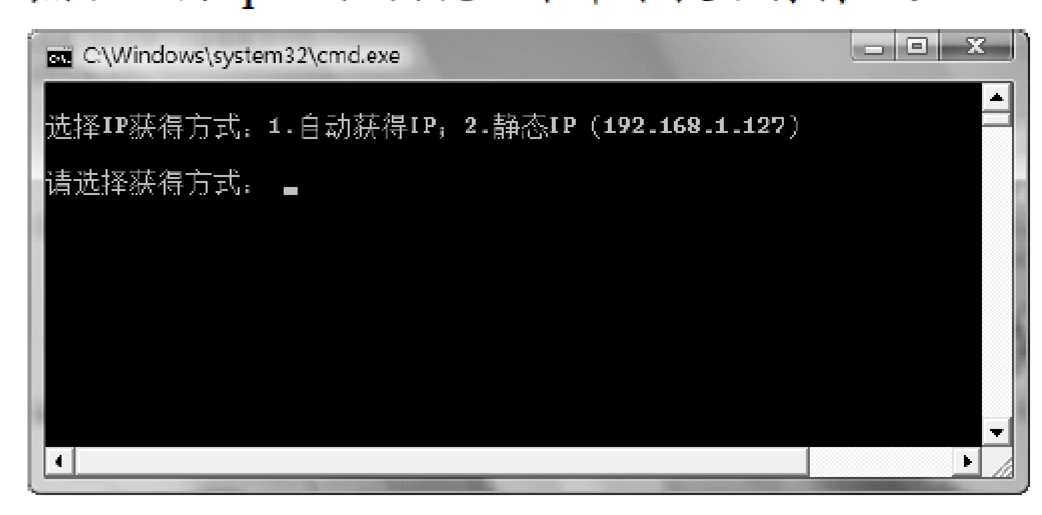
```
@echo off
echo.
echo 选择IP获得方式：1.自动获得IP；2.静态IP (192.168.1.127)
echo.
set sel=
set/p sel=请选择获得方式：
if "%sel%"=="1" goto auto
if "%sel%"=="2" goto static
echo 没有选择IP获得方式。
goto end

:auto
echo 正在更改IP地址......
netsh interface ip set address name="本地连接" source=dhcp
echo 正在更改DNS地址......
netsh interface ip set dns name="本地连接" source=dhcp
echo 自动获得IP更改成功!
goto end

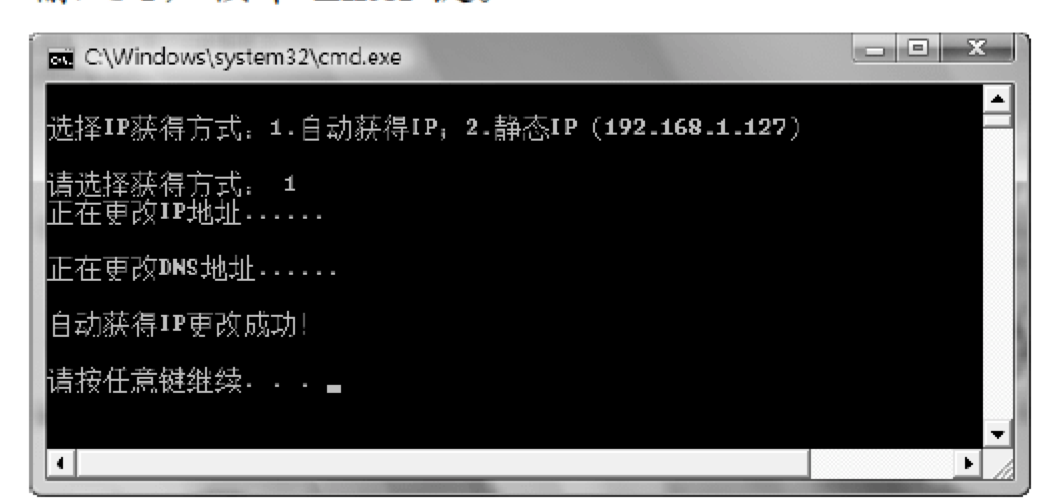
:static
echo 正在更改IP地址......
netsh interface ip add address "本地连接" 192.168.1.127 255.255.255.0 192.168.1.1
echo 正在更改DNS地址......
netsh interface ip add dns "本地连接" 192.168.1.1
echo 设置静态IP成功!
goto end

:end
echo. & pause
```

❷ 将文件另存为后缀名为.bat 的批处理文件，如 ip.bat。然后双击 ip.bat，出现一个命令提示符窗口。



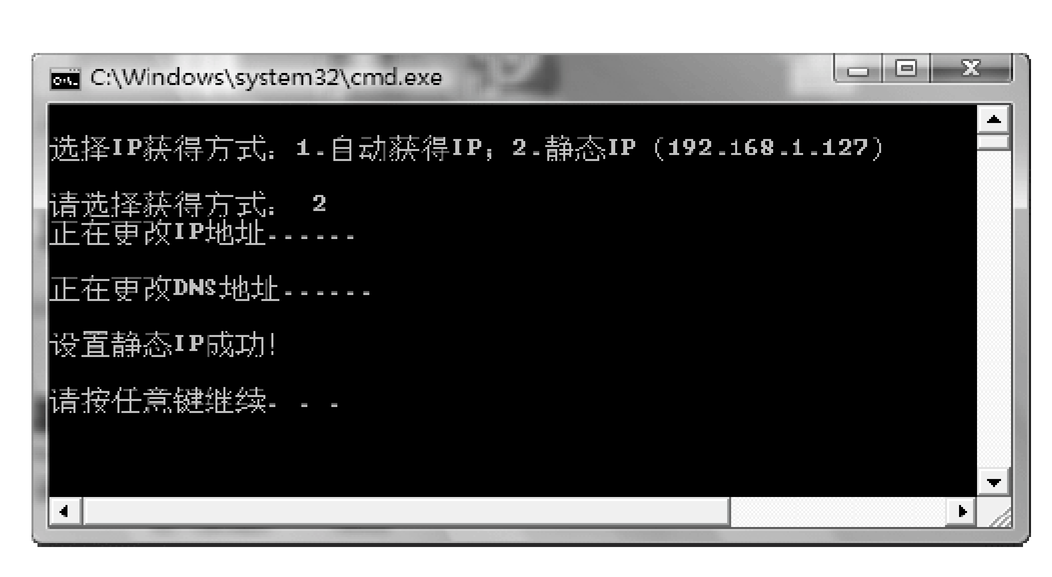
❸ 输入 1，按下 Enter 键。



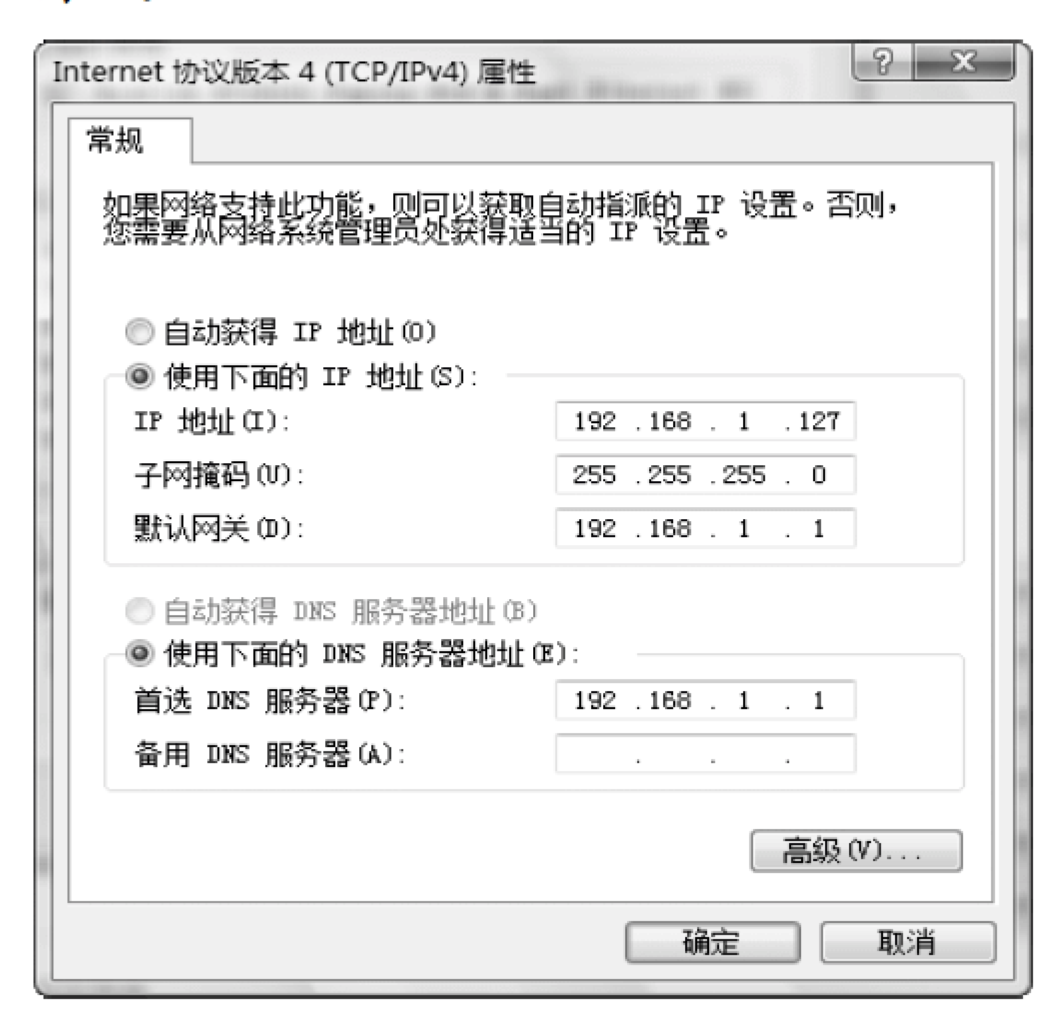
❹ 查看本地连接属性，IP 地址的获得方式变为自动获得。



❺ 输入 2，按下 Enter 键。



❻ 查看本地连接属性，IP 地址变为批处理命令中指定的 IP。



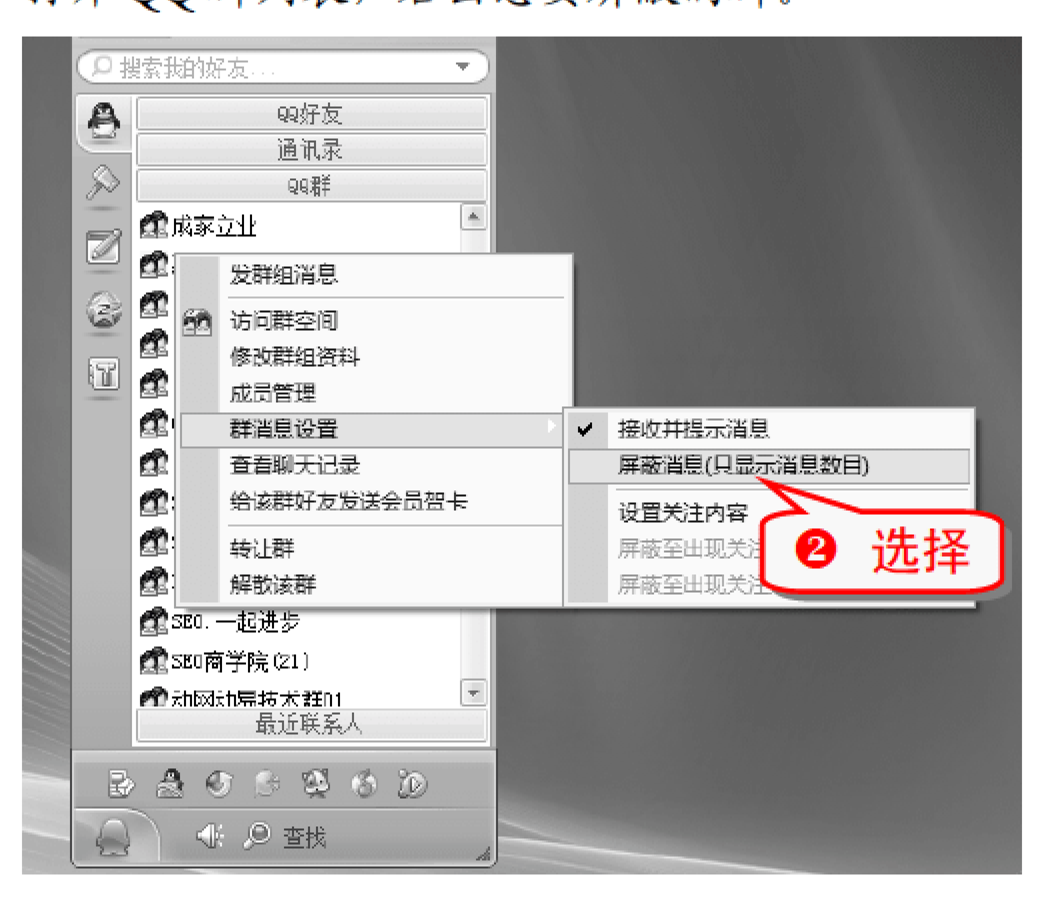
专　家　坐　堂

代码中的 IP 地址可以更改为别的 IP 地址。

技巧176　巧避群消息的骚扰

当用户正忙于工作或学习，却又不想错过群消息时，可以将群消息设置为“屏蔽消息(只显示消息数目)”状态。

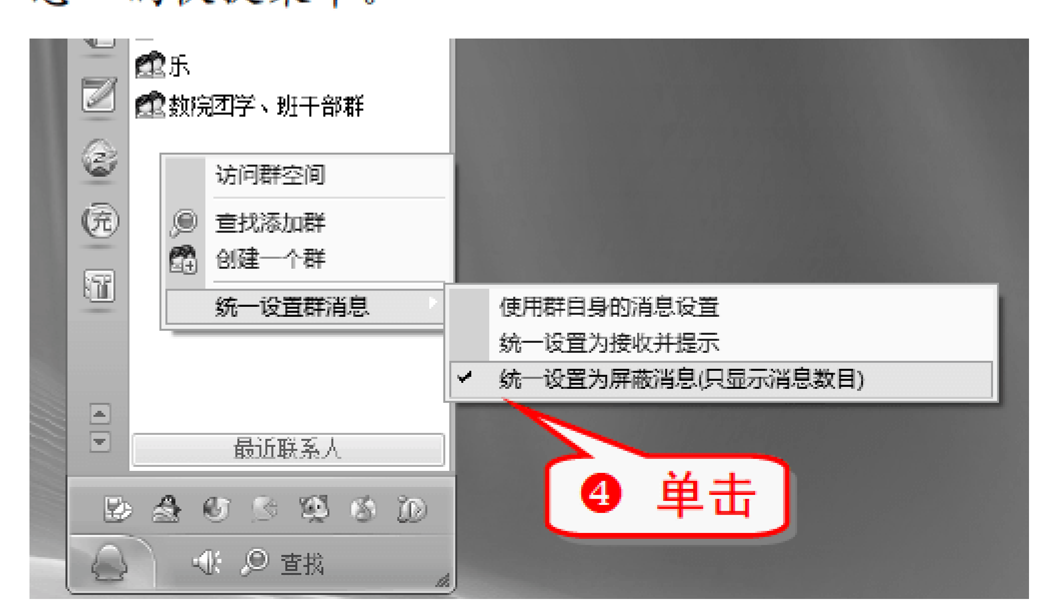
❶ 打开 QQ 群列表，右击想要屏蔽的群。



举　一　反　三

如果群比较多，一个一个设置比较繁琐，可以选择统一设置群消息。

❸ 在群列表最下面的空白处右击，弹出“统一设置群消息”的快捷菜单。

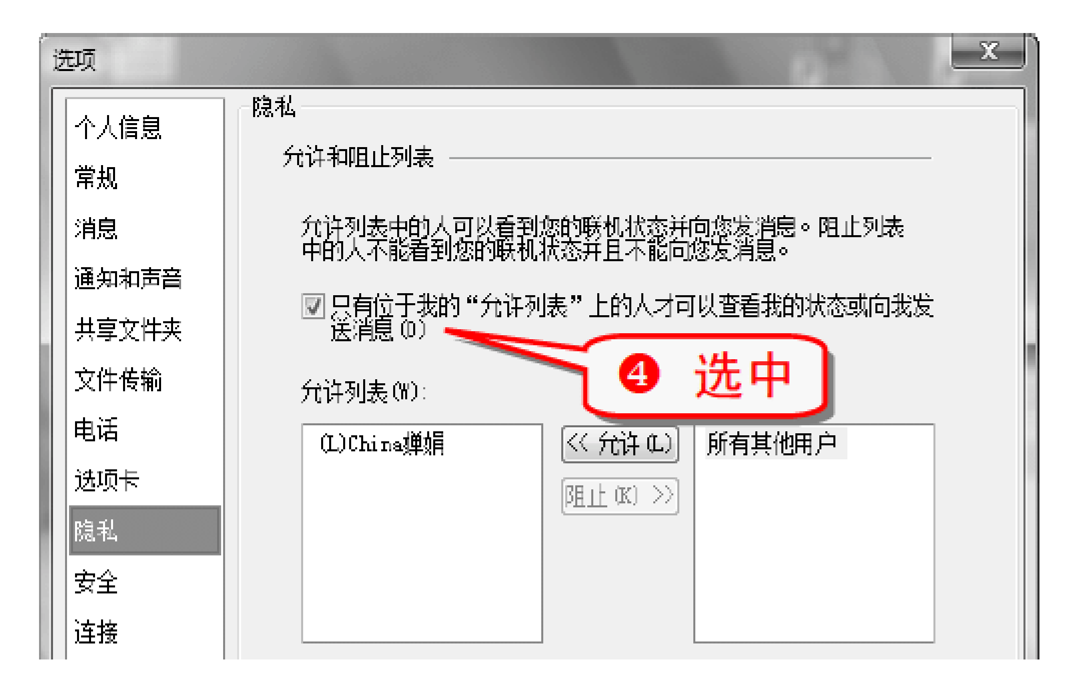


技巧177　防止他人骚扰 MSN

在使用 MSN 的时候为了防止骚扰，可以将其设置为只有经过允许他人才可以向当前用户发送消息。

❶ 打开 MSN。







❺ 在“允许列表”中添加允许查看我的状态或向我发送消息的用户的名单，单击“确定”按钮。

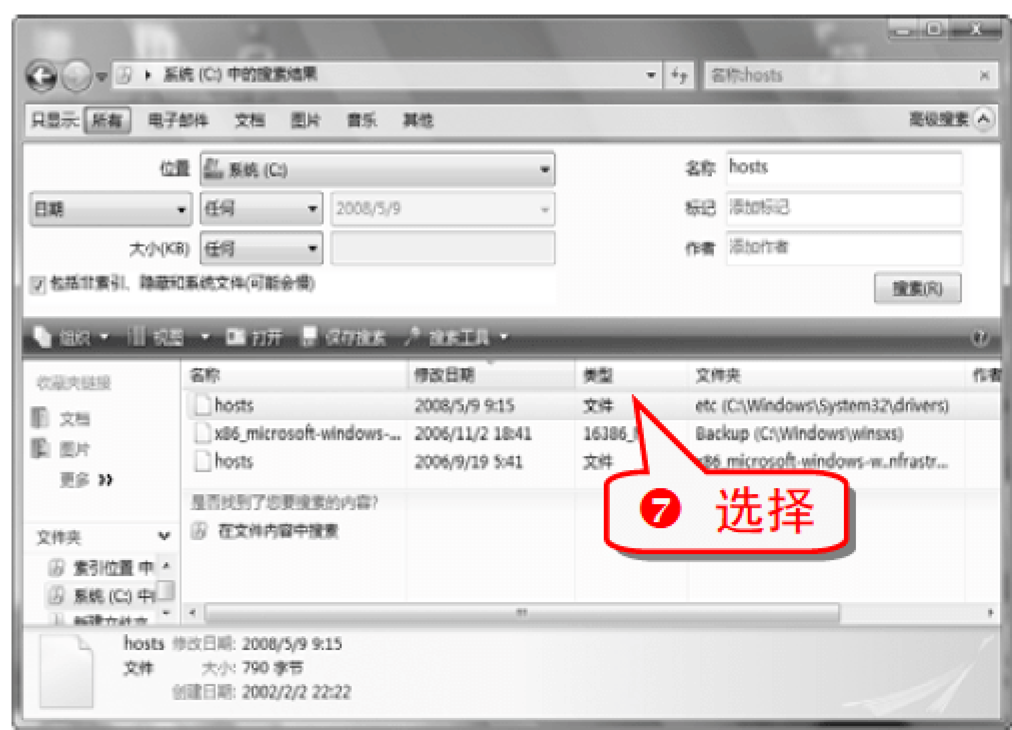
技巧178　巧用 hosts 文件屏蔽恶意网站

在 Windows Vista 系统中存在一个名为 hosts 的文件，可以利用其屏蔽已知的恶意网站，这里用 www.163.com 网址举例说明。

(1) 搜索 C 盘的 hosts 文件

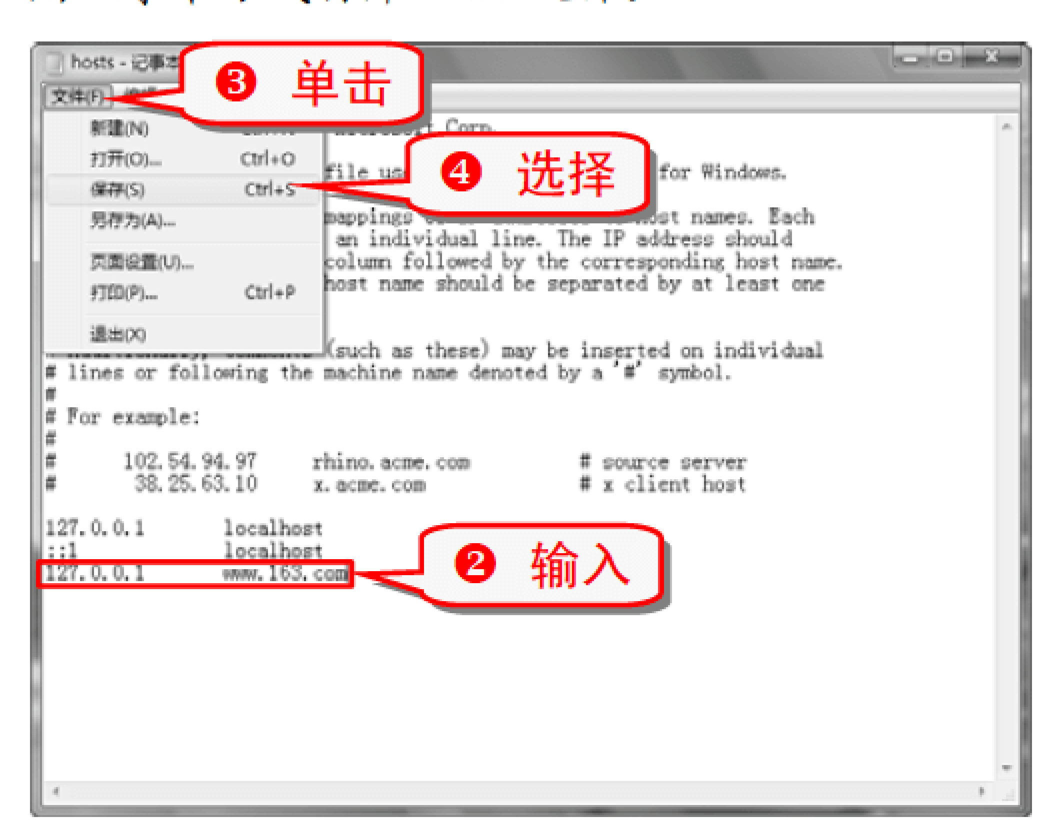
❶ 选择“开始”→“搜索”命令。





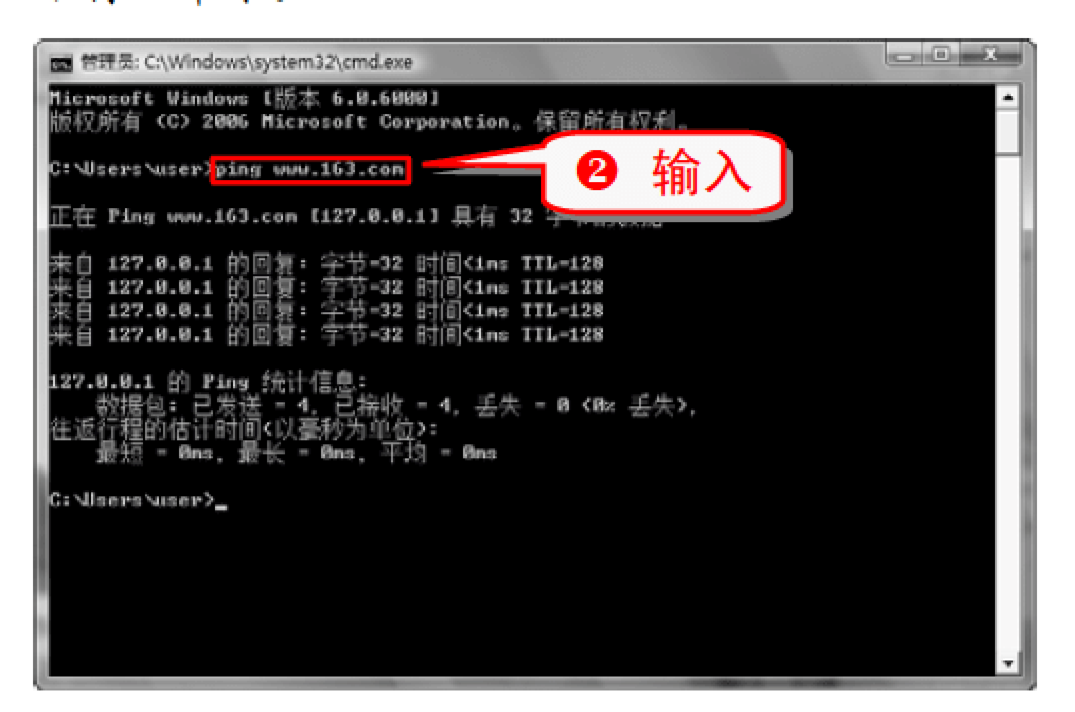
(2) 修改 hosts 文件屏蔽网站

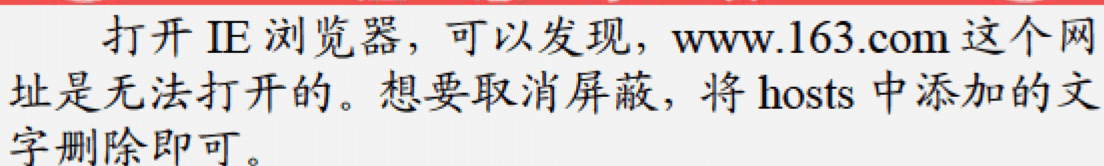
❶ 用记事本方式打开 hosts 文件。



(3) 验证网站是否屏蔽成功

❶ 选择“开始”→“所有程序”→“附件”→“命令提示符”命令。





打开 IE 浏览器，可以发现，www.163.com 这个网址是无法打开的。想要取消屏蔽，将 hosts 中添加的文字删除即可。

技巧179　恢复被修改的 IE 主页

通过安装软件或是访问到恶意网页都有可能导致 IE 主页被修改。这里介绍一种最简单的恢复方法。

❶ 在打开的 IE 浏览器中选择“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框。



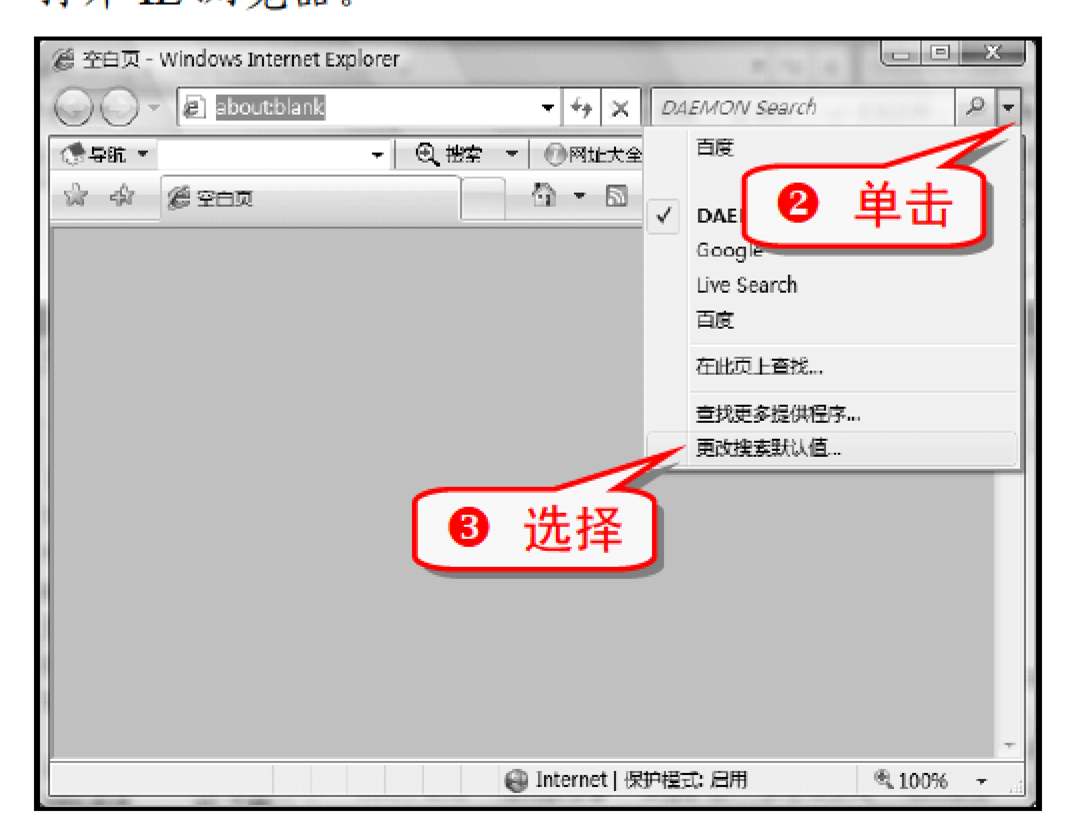
知　识　补　充

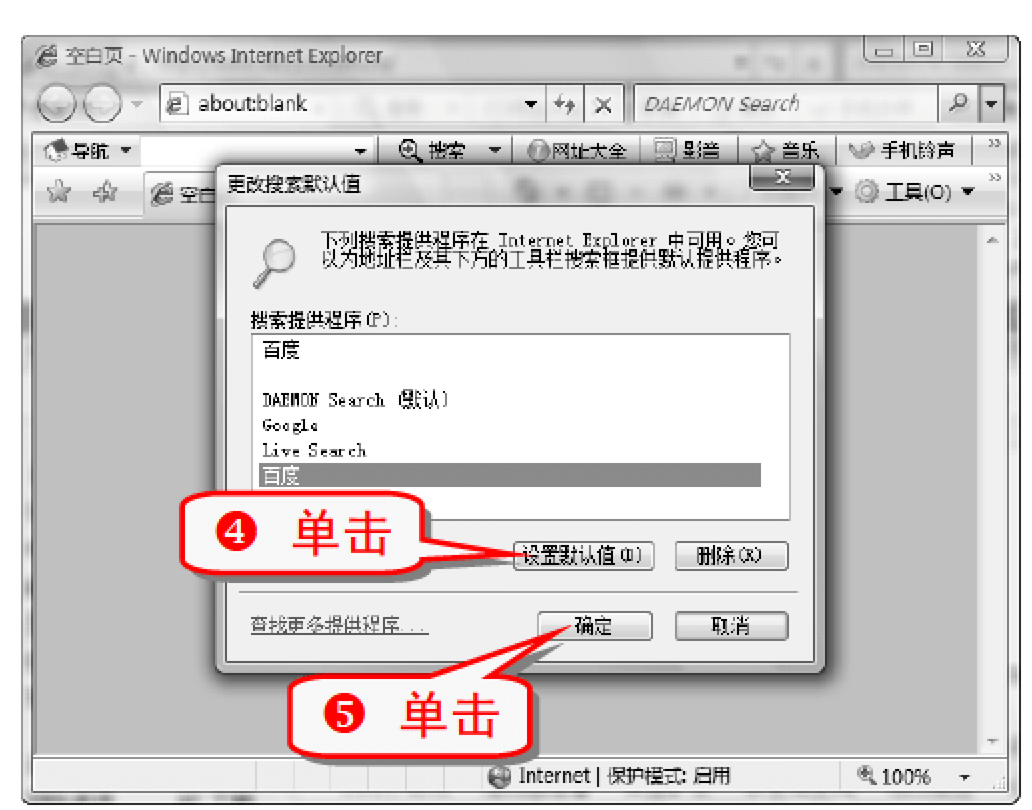
上述步骤只是将百度设置为 IE 主页，也可以将其他常用的网址设置为 IE 主页，或者是将 IE 主页设置为空白页。

技巧180　恢复被修改的 IE 搜索引擎

IE 7.0 的默认搜索引擎是百度，当单击了恶意链接后，可能会修改默认搜索引擎，通过简单的几步设置即可将其修改回默认值。

❶ 打开 IE 浏览器。

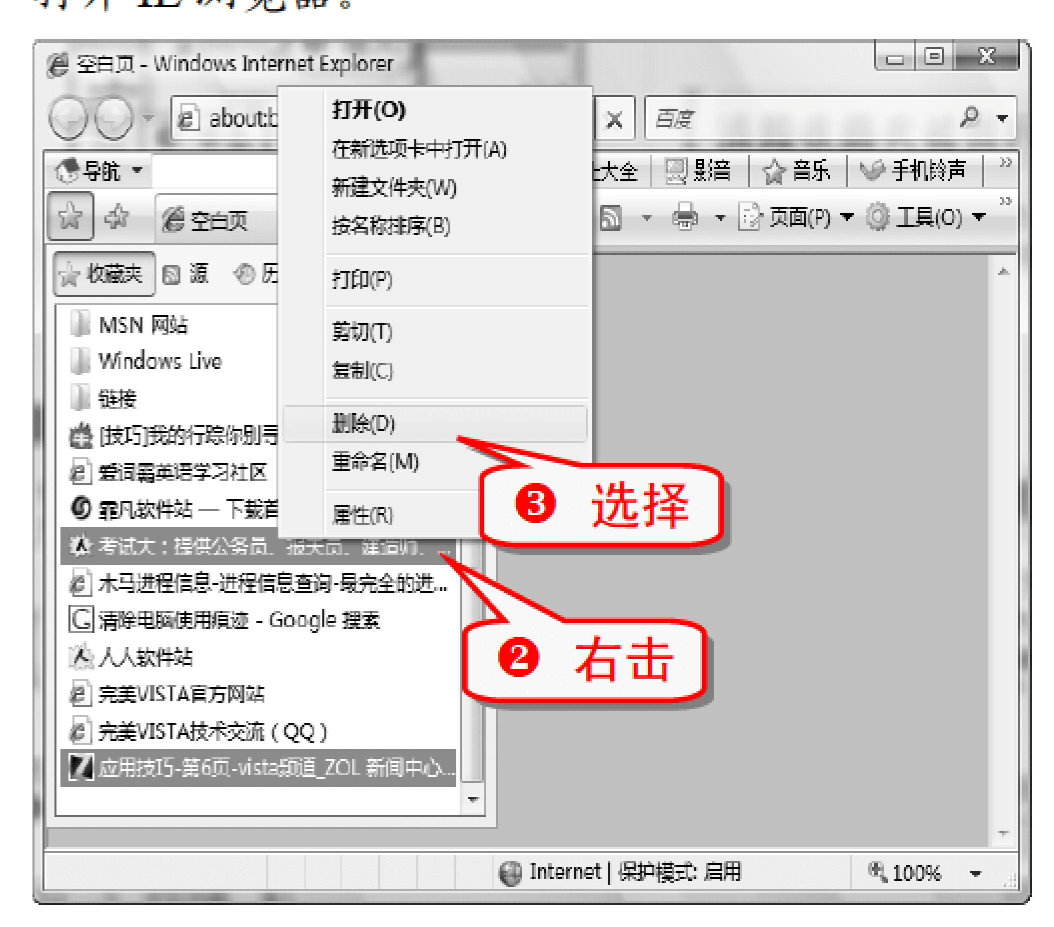




技巧181　清除收藏夹被强行添加的链接

在 IE 浏览器的收藏夹中会出现一些陌生的网站链接，这是有些网站通过修改注册表在 IE 收藏夹中强行添加的。

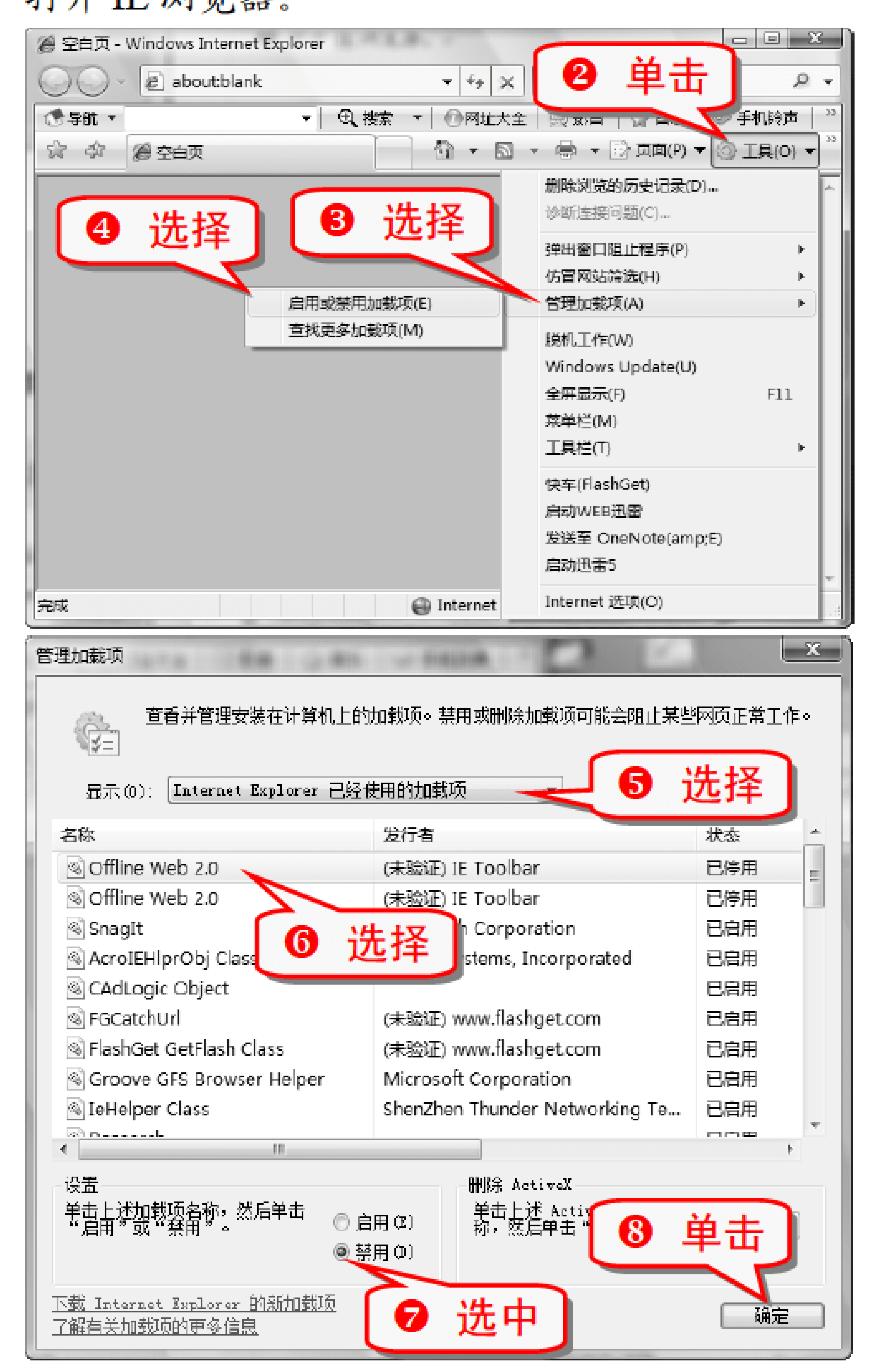
❶ 打开 IE 浏览器。



技巧182　清除被强行添加的 IE 插件

打开 IE 浏览器的时候，发现工具栏上多了一些选项，如 导航 搜索 网址大全 影音 音乐 手机铃声，证明 IE 被强行加载了插件，使用以下方法可清除 IE 插件。

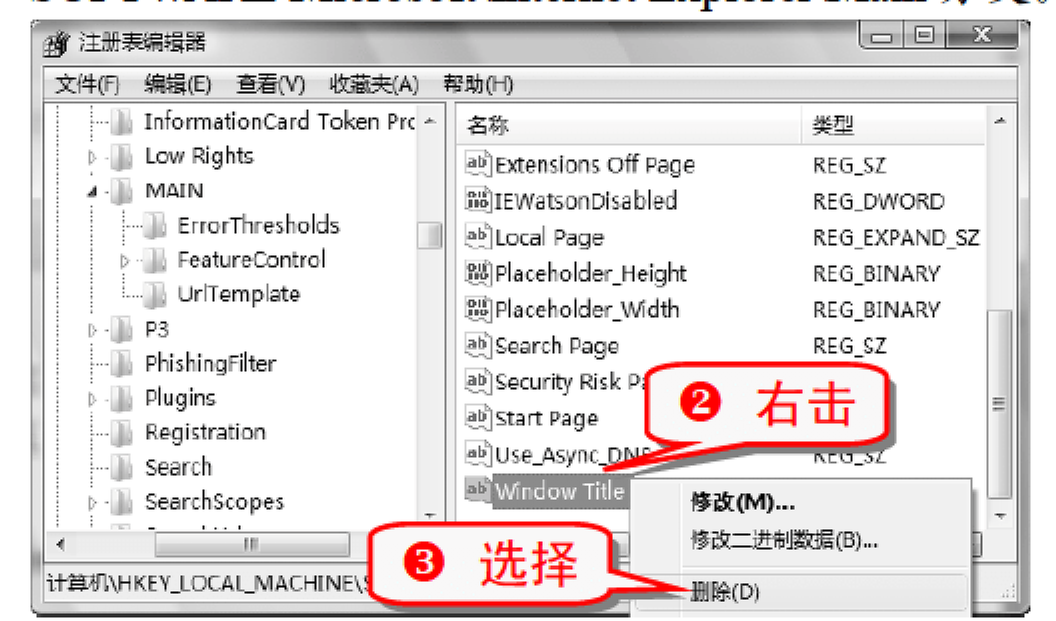
❶ 打开 IE 浏览器。



技巧183　清除 IE 标题栏添加的非法信息

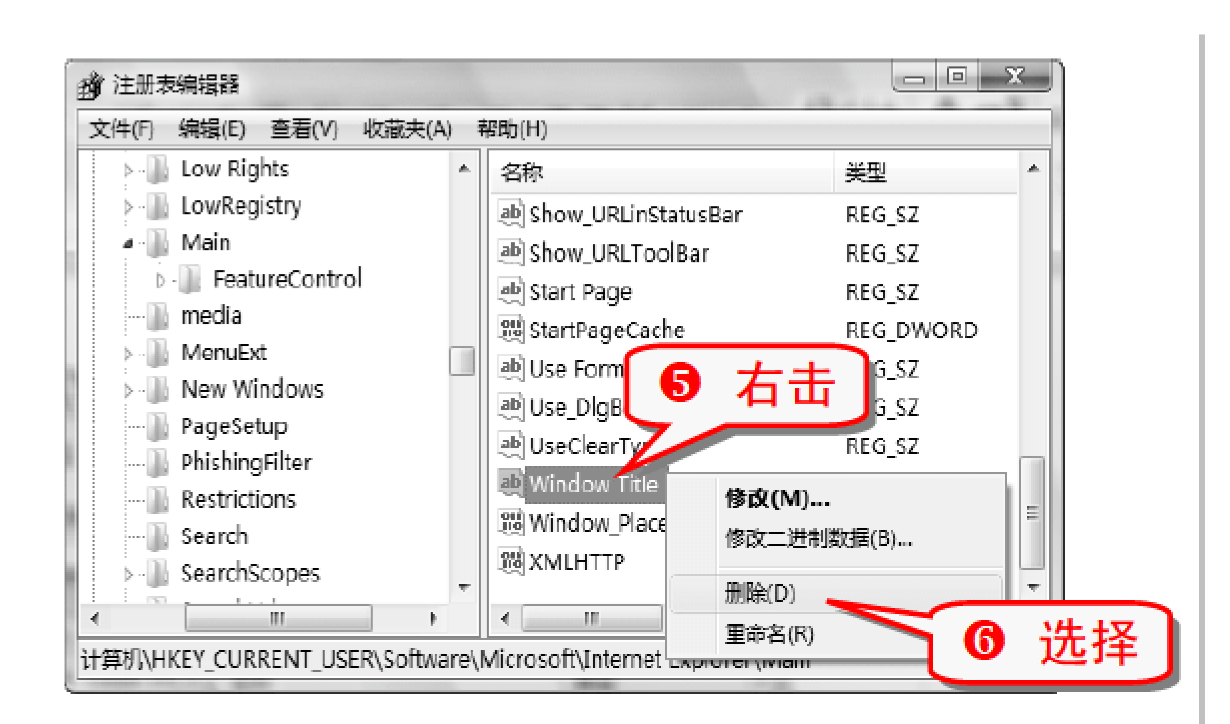
通过修改注册表可以清除 IE 标题栏被添加的非法信息。

❶ 打开注册表编辑器，展开 HKEY_LO CAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main 分支。



❹ 展开 HKEY_CURRENT_ USER\Software\Microsoft\InternetExplorer\Main 分支。





技巧184　清除 IE 地址栏中的文字信息

浏览网站时，有些恶意网站会自动将 IE 地址栏中的常用网址覆盖并添加文字信息，可以通过修改注册表来清除 IE 地址栏中的文字信息。

❶ 打开注册表编辑器，展开 HKEY_CURR ENT_USER\Software\Policies\Microsoft\InternetExplorer\Toolbar 分支。

❷ 选择 LinksFolderName 选项并双击。

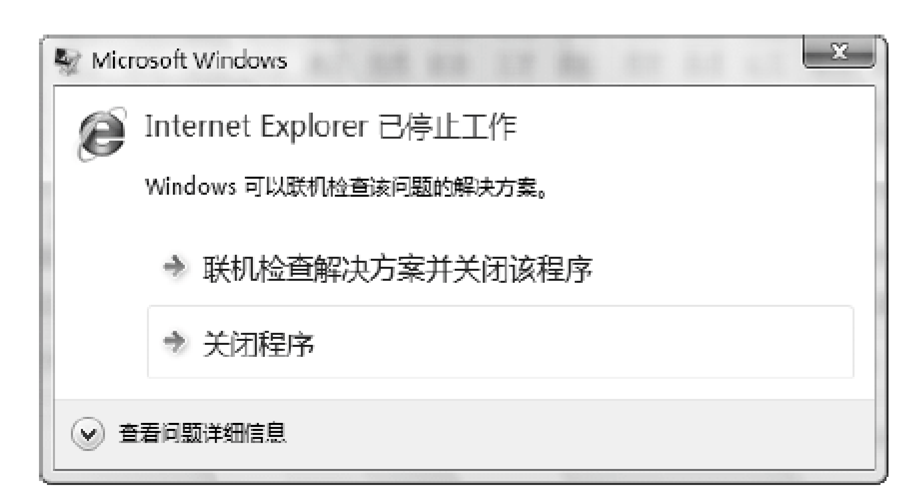


技巧185　解决超级兔子加载项引发的 IE 问题

在浏览网页的时候，网页突然变成白色，一段时间后所有打开的网页自动关闭了。如图所示，鼠标显示正忙的状态。



过一段时间弹出如下警告框。



使用杀毒软件扫描不出任何问题，查看系统进程也没有发现可疑之处，只剩下插件问题。

❶ 打开 IE 浏览器。





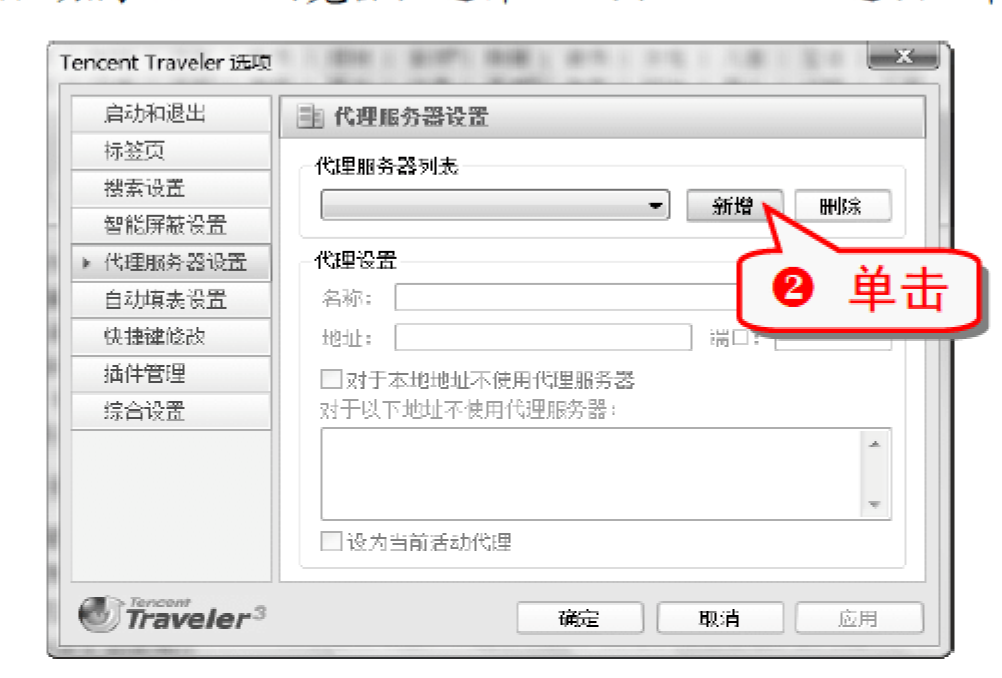
❹ 发现两个未验证的“超级兔子上网精灵”加载项呈启动状态，将其禁用。



技巧186 为 TT 上网穿上隐身衣

使用代理服务器上网，在浏览网页的时候其他用户就不能通过显示 IP 的方法找到真实的 IP 地址，达到“隐身”的效果。

❶ 启动腾讯 TT 浏览器，选择“工具”→“TT 选项”命令。





专家坐堂

免费的代理服务器可以在网上找到，http://www.proxycn.com/是一个比较好的提供免费代理服务器的网站。

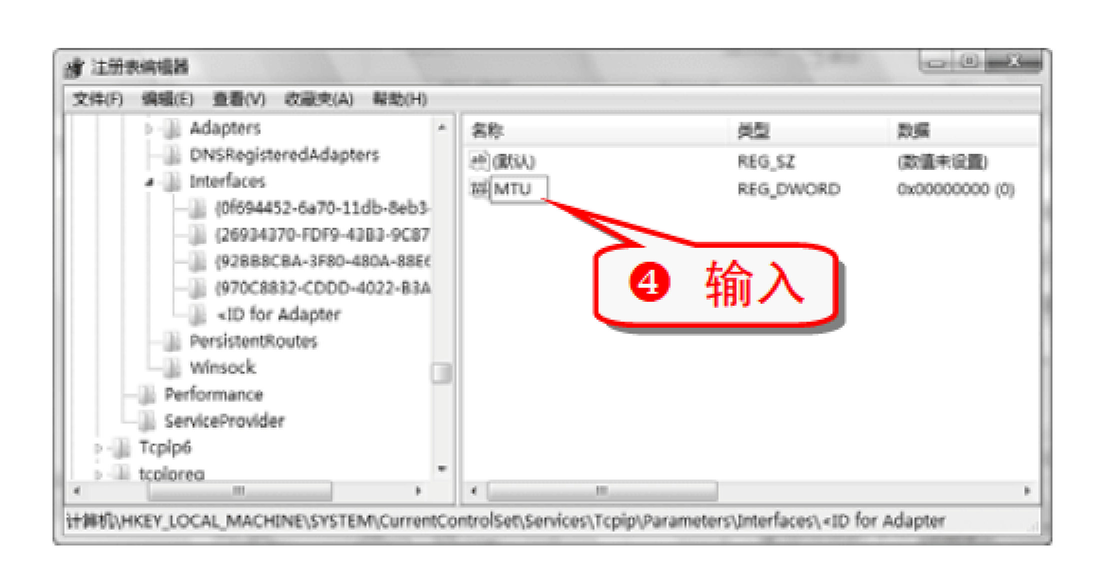
技巧187 使代理上网恢复正常浏览

电信用户使用 ADSL 代理上网时会出现无法正常浏览某些网页的问题，可以通过修改注册表来解决此问题。

❶ 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<ID for Adapter 分支。

❷ 选择<ID for Adapter 选项并在右边窗格的空白处右击。





❺ 选中 MTU 选项并双击。

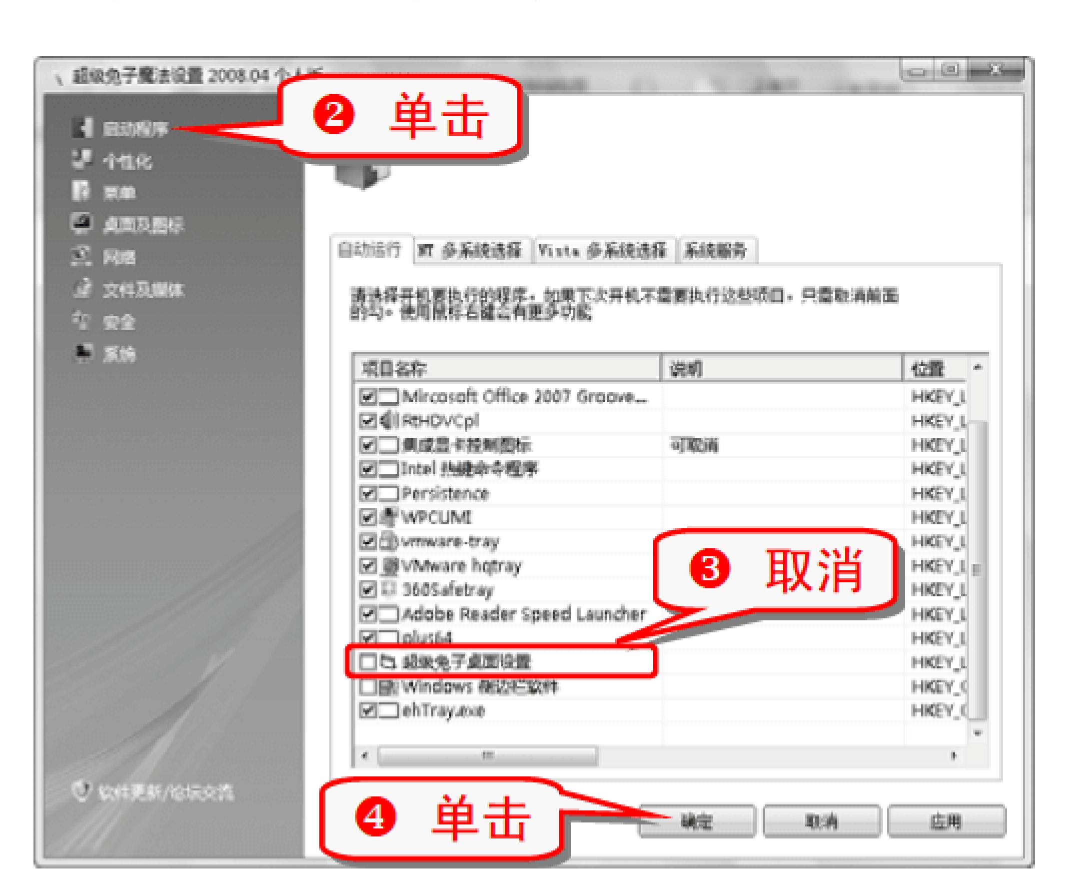


技巧188 巧用超级兔子

超级兔子魔法设置可以提供系统隐藏参数，调整系统，使其更适合用户的需求。

(1) 快速管理启动项

❶ 运行“超级兔子”应用程序，在弹出的“超级兔子”对话框中，单击“打造属于自己的系统”链接，弹出“超级兔子魔法设置”对话框。



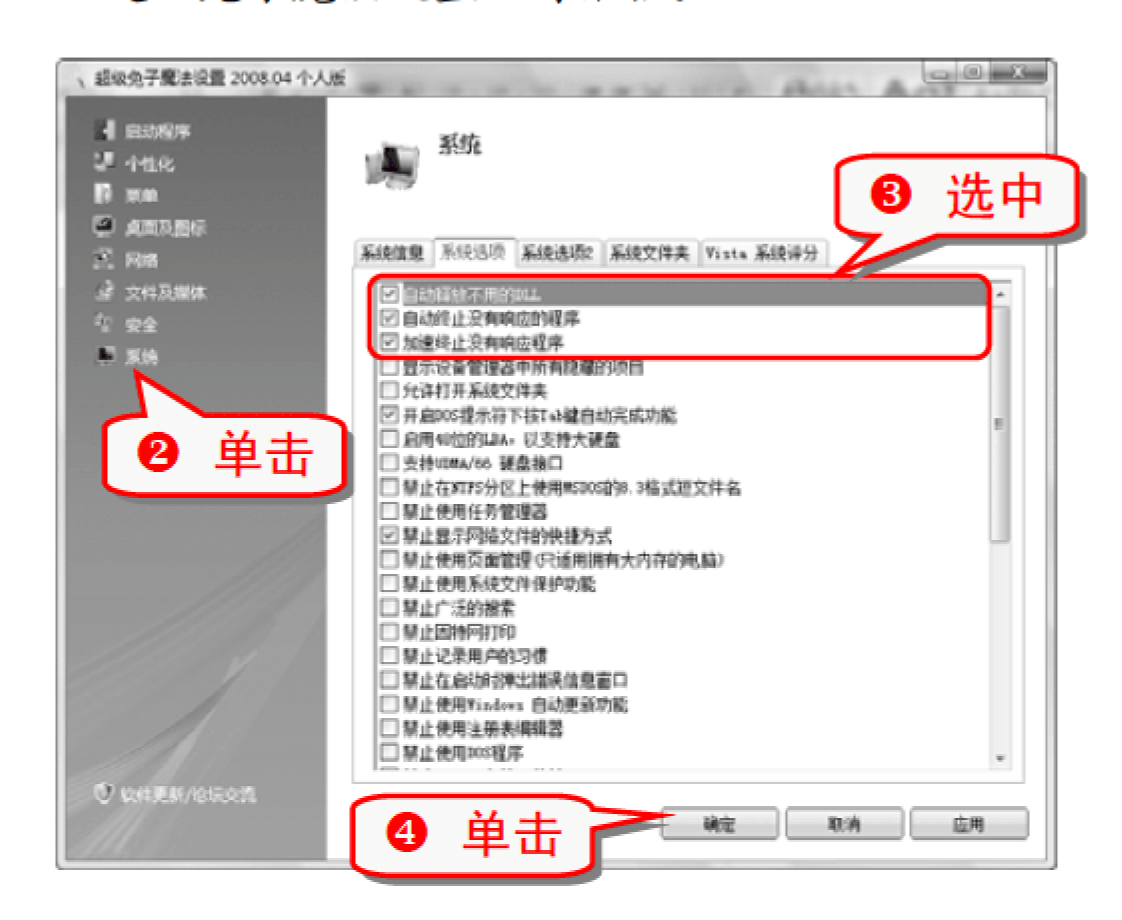
知识补充

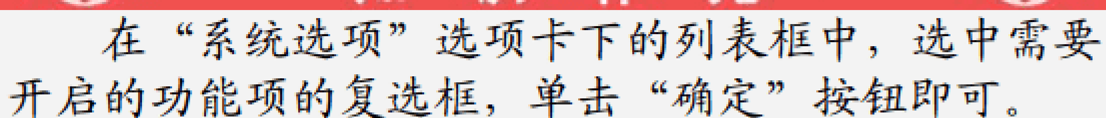
在“自动运行”选项卡下的列表框中，取消选中应用程序的复选框，这样在启动系统时，这些应用程序就不会随系统一起启动，从而加快系统的启动速度。



(2) 优化系统选项

❶ 运行“超级兔子”应用程序，在弹出的“超级兔子”对话框中，单击“打造属于自己的系统”链接，弹出“超级兔子魔法设置”对话框。





知 识 补 充

在“系统选项”选项卡下的列表框中，选中需要开启的功能项的复选框，单击“确定”按钮即可。

举 一 反 三

在超级兔子魔法设置中，还可以对系统的个性化、菜单、桌面及图标、网络、文件及媒体和安全进行优化设置，这些设置都相对比较简单，用户可以根据需要进行设置。

(3) 一键修复 IE

使用超级兔子的一键修复 IE 功能项可以帮助用户快速修复出错的 IE，检测 IE 是否被加载了恶意插件和木马等。

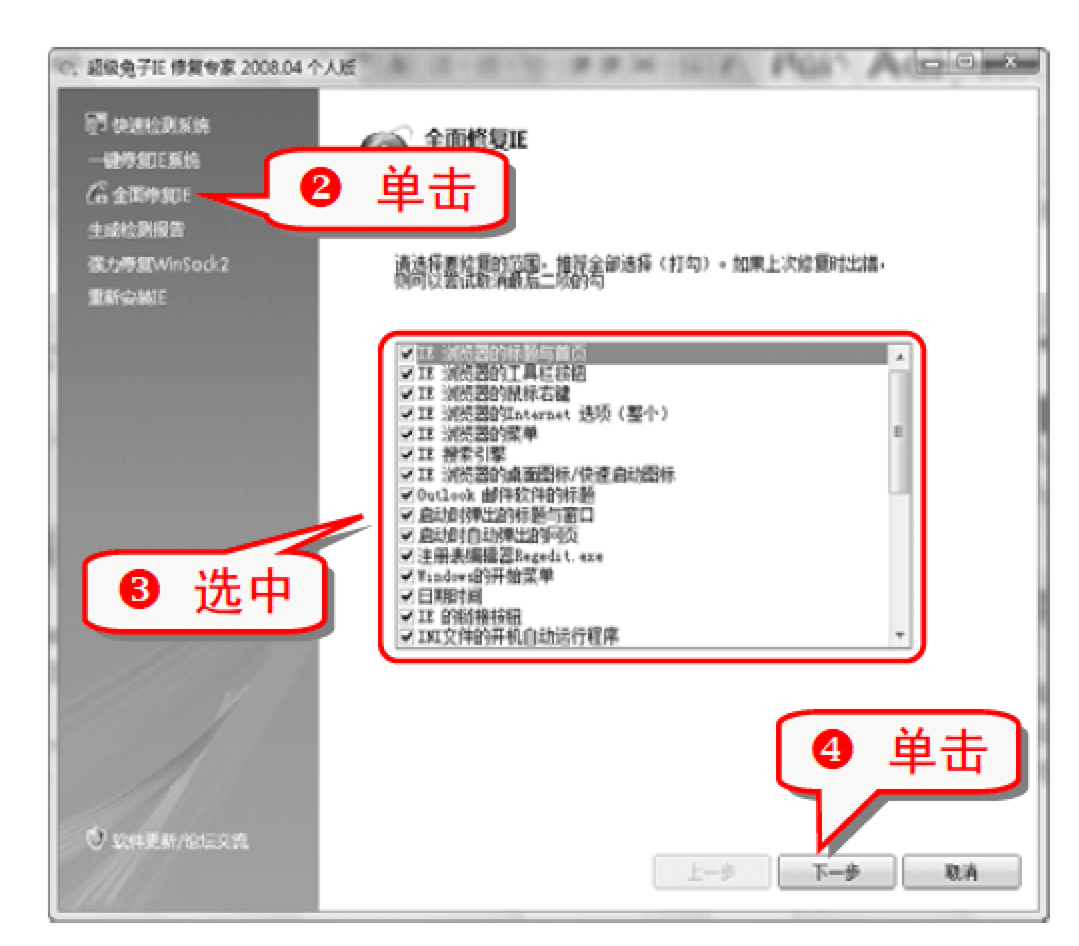
❶ 运行“超级兔子”应用程序，在弹出的“超级兔子”对话框中，单击“修复 IE、检测木马”链接，弹出“超级兔子 IE 修复专家”对话框。



(4) 全面修复 IE

全面修复 IE，能够识别很多恶意网站的病毒，并给予清除。

❶ 运行“超级兔子”应用程序，在弹出的“超级兔子”对话框中，单击“修复 IE、检测木马”链接，弹出“超级兔子 IE 修复专家”对话框。





❻ 修复完成后，单击“完成”按钮即可。



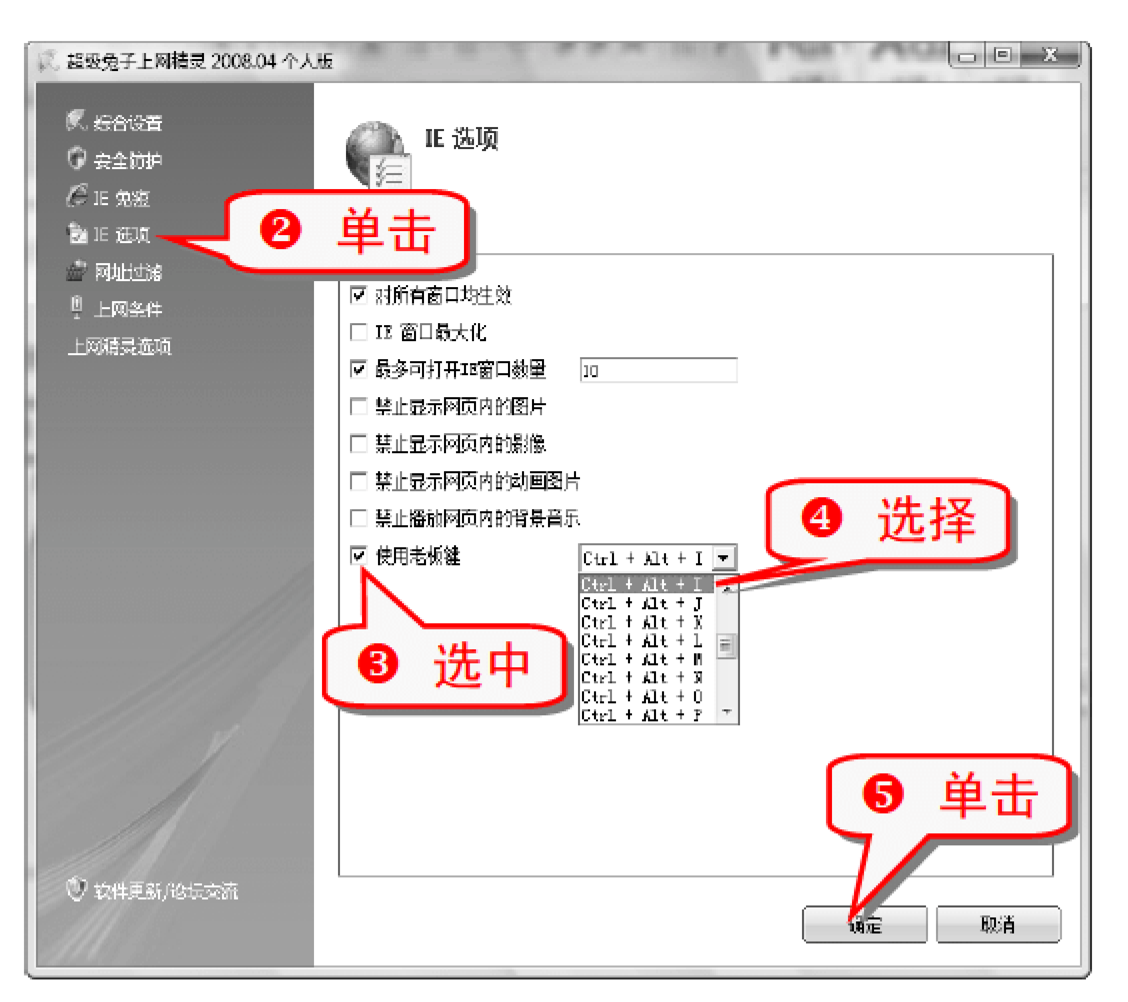
注 意 事 项

修复完成后，重新启动电脑，如果没有修复成功再依次执行修复操作。

(5) 使用老板键隐藏 IE

使用超级兔子上网精灵可以快速实现隐藏 IE 的功能。

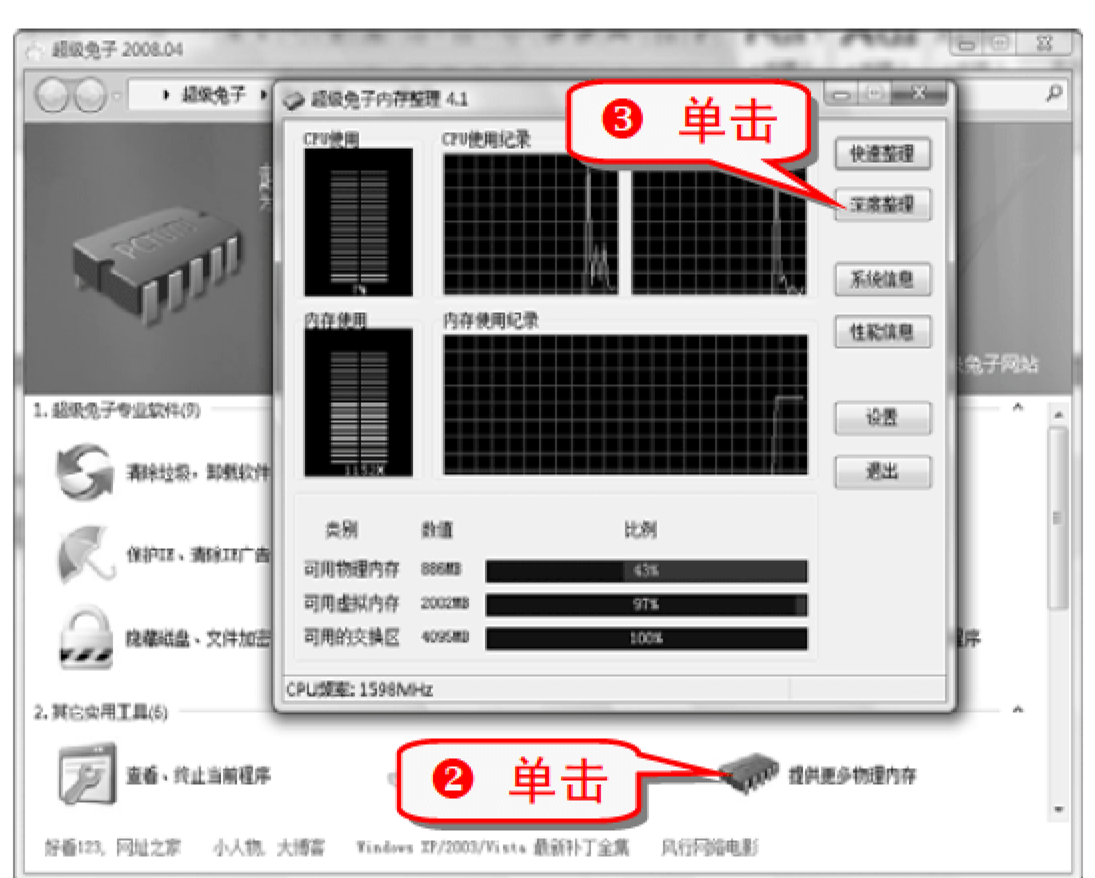
❶ 运行“超级兔子”应用程序，在弹出的“超级兔子”对话框中，单击“保护 IE、清除 IE 广告”链接，弹出“超级兔子上网精灵”对话框。



(6) 超级兔子内存整理功能

使用超级兔子的内存整理功能，可以为应用软件提供更多的物理内存，提高系统的运行效率。

❶ 运行“超级兔子”应用程序，弹出“超级兔子”对话框。







(7) 更强大的任务管理器

超级兔子提供的任务管理器比系统自带的功能更强大，可以管理窗口、进程、模块以及端口。

❶ 运行“超级兔子”应用程序，在弹出的“超级兔子”对话框中，单击“查看、终止当前程序”链接，弹出“超级兔子任务管理器”对话框。



技巧189　巧用 360 保险箱保护网上银行账户

360 保险箱是 360 安全中心推出的账号密码安全保护软件，采用主动防御技术，可以阻止盗号木马对网游、聊天等程序的侵入。

❶ 选择“帐号保护”→“网络银行”命令。







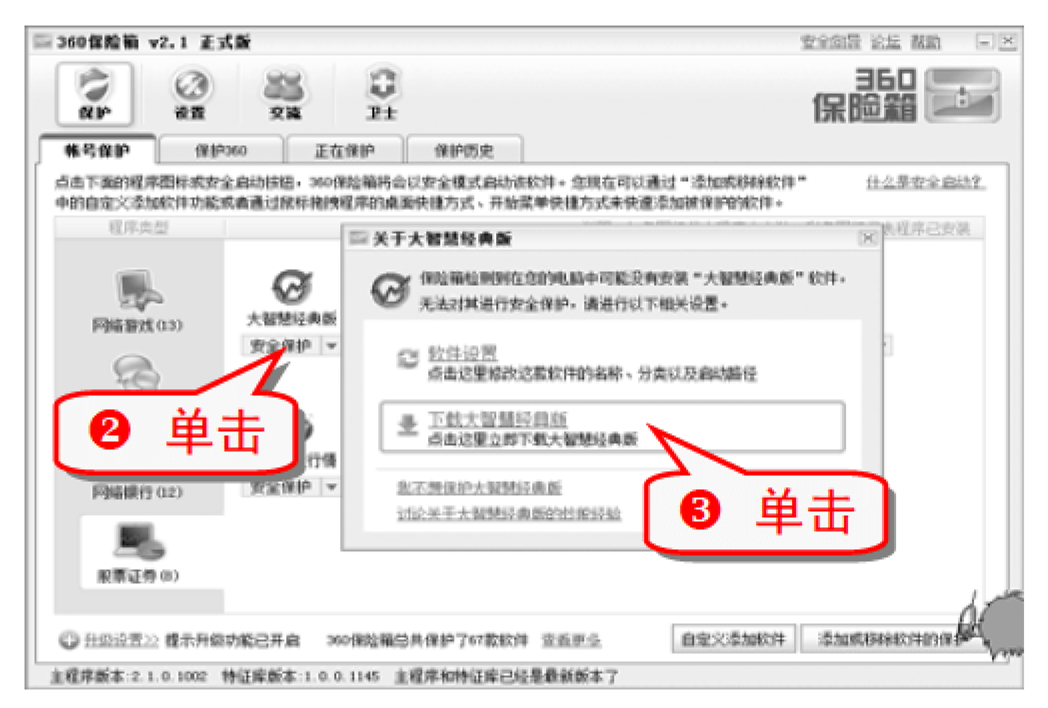
专 家 坐 堂

通过上述步骤，工商银行的主页在安全模式下打开，在其后的整个操作过程中都受到 360 保险箱的保护。

技巧190　巧用 360 保险箱保护网上炒股账户

360 保险箱不仅可以保护网上银行账户，还可以保护网上炒股软件的账户。

❶ 选择“帐号保护”→“股票证券”命令，查看是否正确安装了炒股软件。



❹ 浏览器链接到华军软件园网站，可以放心进行下载。

❺ 安装后，主界面中该程序图标变成彩色的，直接单击就可以安全使用。

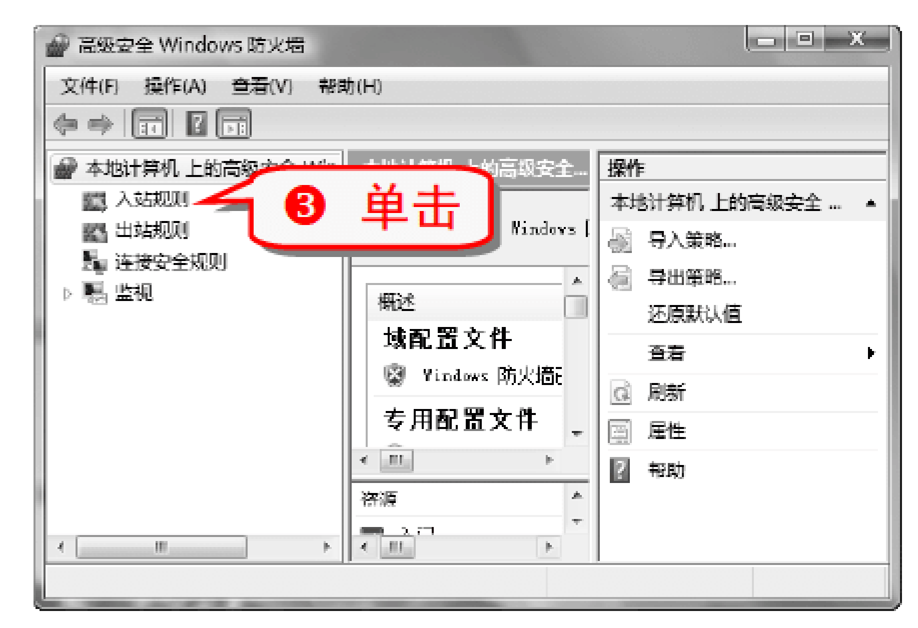
技巧191　巧用系统自带的防火墙

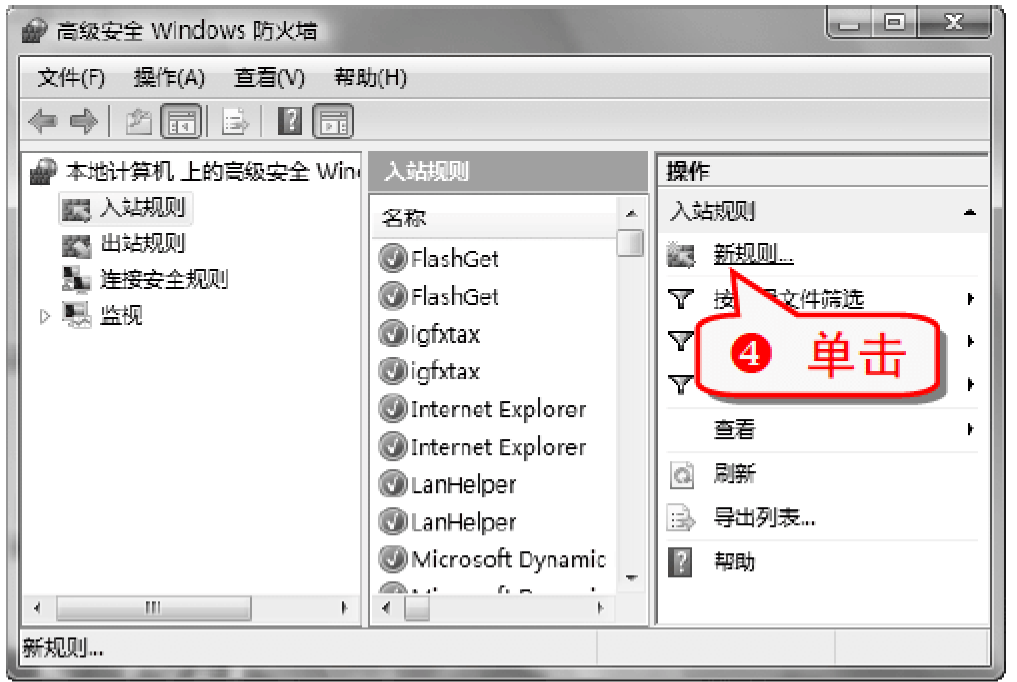
Windows Vista 系统下自带的防火墙功能很强大，巧用该防火墙的功能可以提高网络访问的安全性。

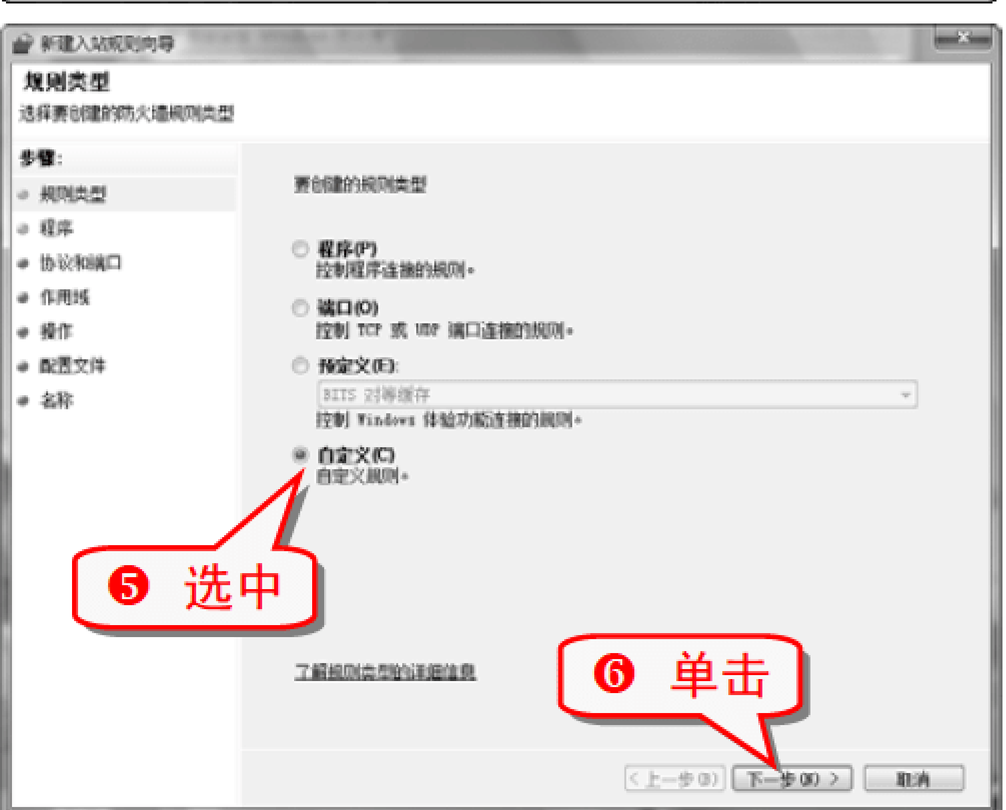
(1) 防止被 Ping

❶ 选择“开始”→“控制面板”命令，打开“控制面板”窗口，双击“管理工具”图标。

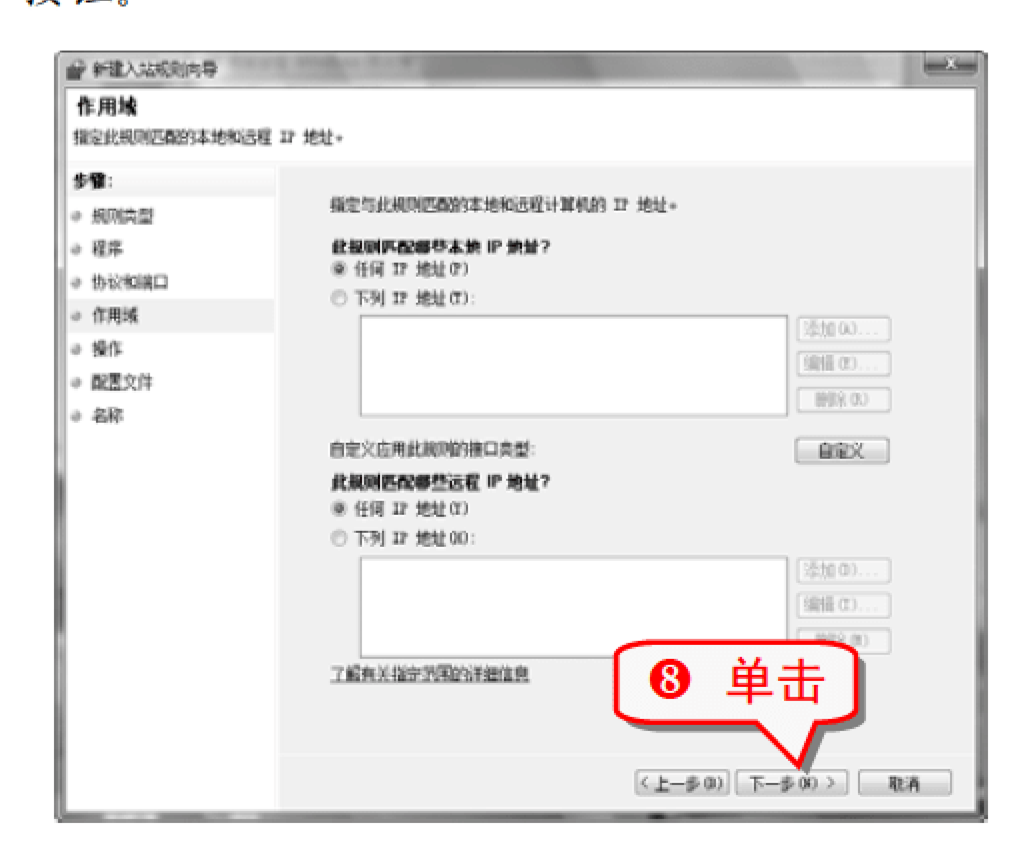








❼ 在对话框中选中“所有程序”选项，单击“下一步”按钮。然后选择协议类型为 ICMPv4，单击“下一步”按钮。





❿ 单击“下一步”按钮，转到“配置文件”设置对话框。单击“下一步”按钮，转到“名称”设置对话框，输入一个合适的名称，单击“完成”按钮。

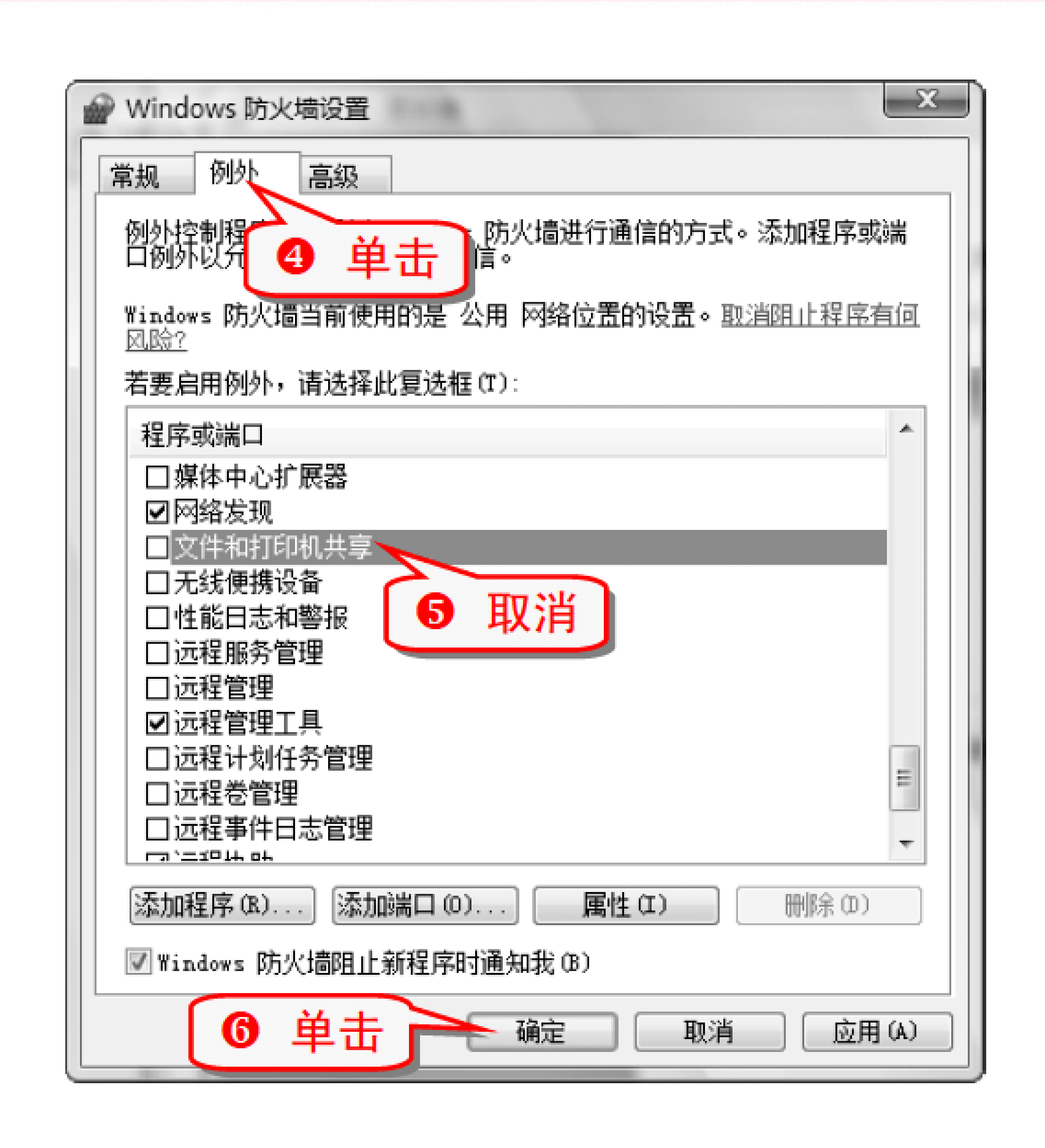
(2) 保护网络打印安全

系统防火墙可以禁止用户通过网络使用共享打印机。

❶ 选择“开始”→“网络”命令，打开“网络”窗口。单击“网络和共享中心”选项，打开“网络和共享中心”窗口。



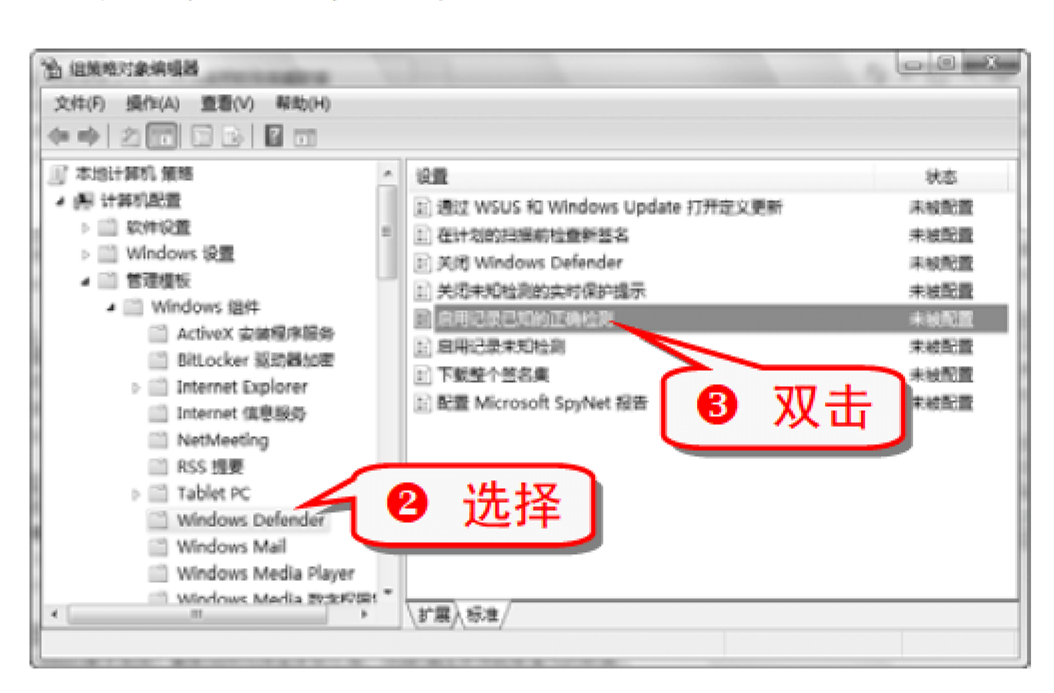


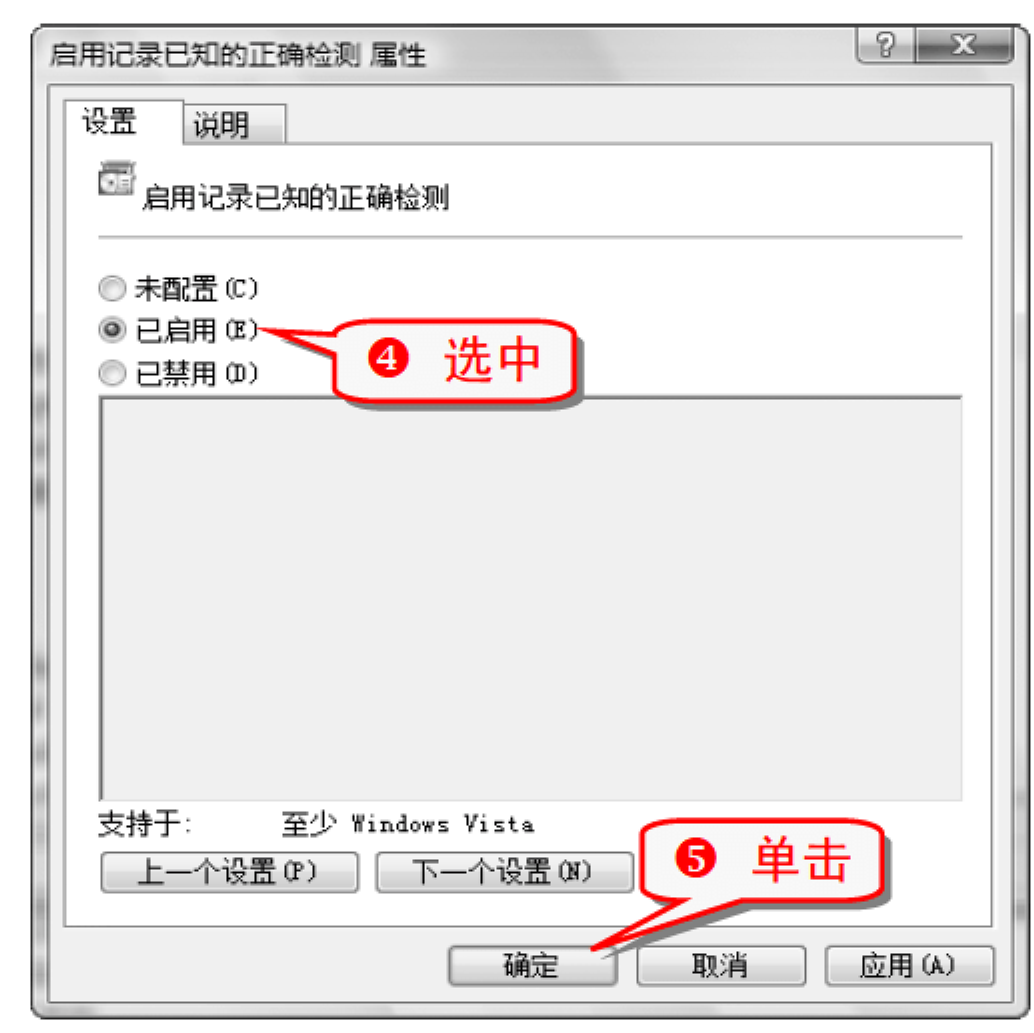


(3) 记录非法攻击痕迹

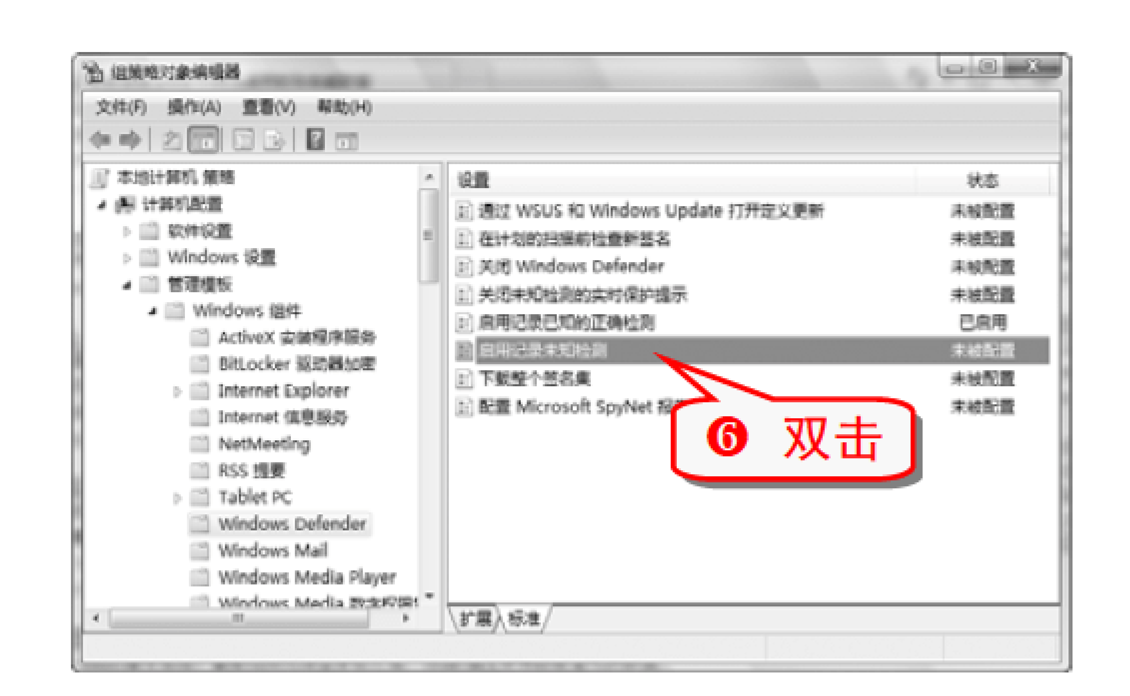
启用防火墙的记录功能可以将任何攻击当前电脑的痕迹都记录下来。

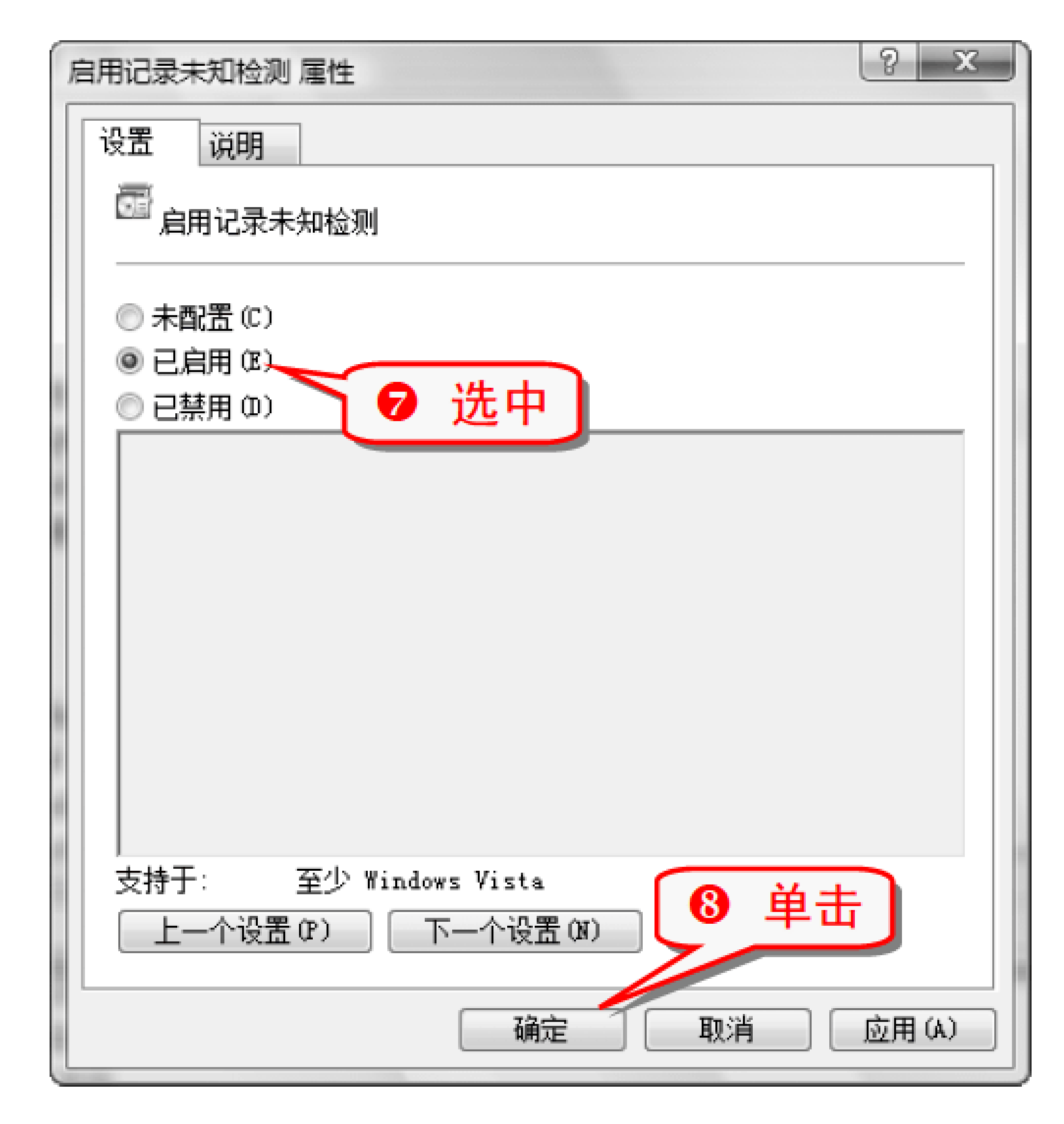
❶ 打开组策略对象编辑器。






举一
反三


❻ 双击

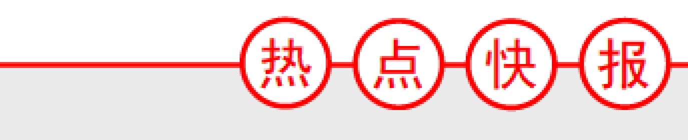

启用记录未知检测 属性
设置
说明
启用记录未知检测
未配置(C)
已启用(E)
已禁用(D)
❼ 选中
支持于:
至少 Windows Vista
上一个设置(P)
下一个设置(N)
❽ 单击
确定
取消
应用(A)



专题七　做好黑客安全防护

内容导航

黑客攻击无处不在，木马和病毒也无处不在，在不断地忙着查毒和杀毒的同时，不要忘了做好防御黑客的工作。只有预防为主，才能依靠防治结合打造一个安全的系统。

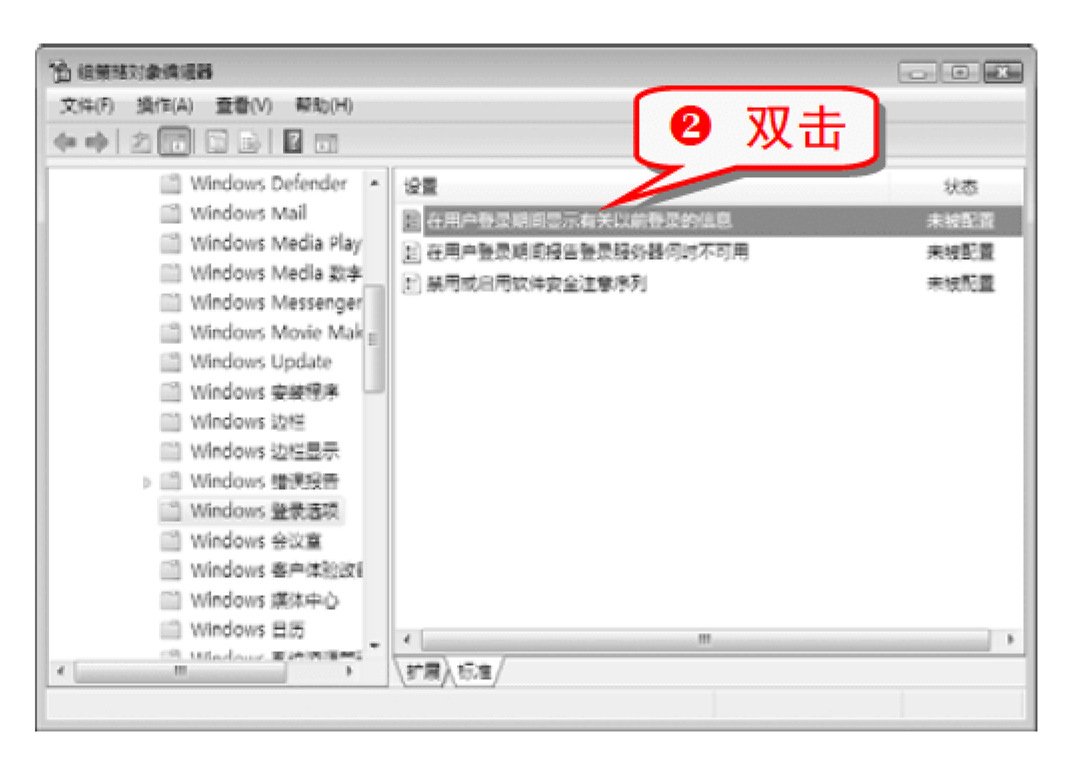


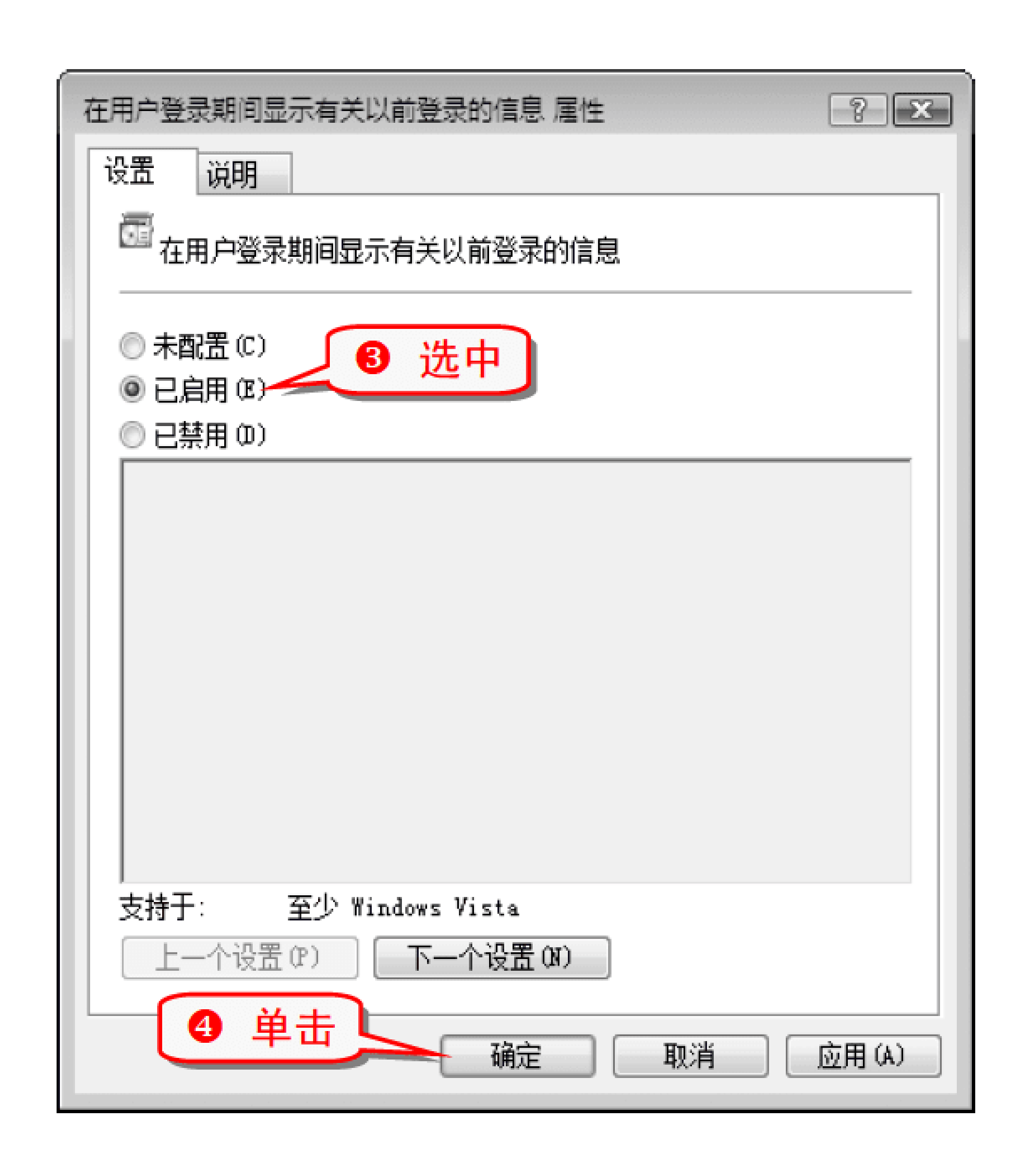
- 记录系统登录时间
- 设置 ARP 缓存老化
- 防范 IPC$入侵
- 禁止发布共享文件夹
- 关闭多余的协议
- 预防图片病毒的侵害

技巧192　使系统记录上一次的登录时间

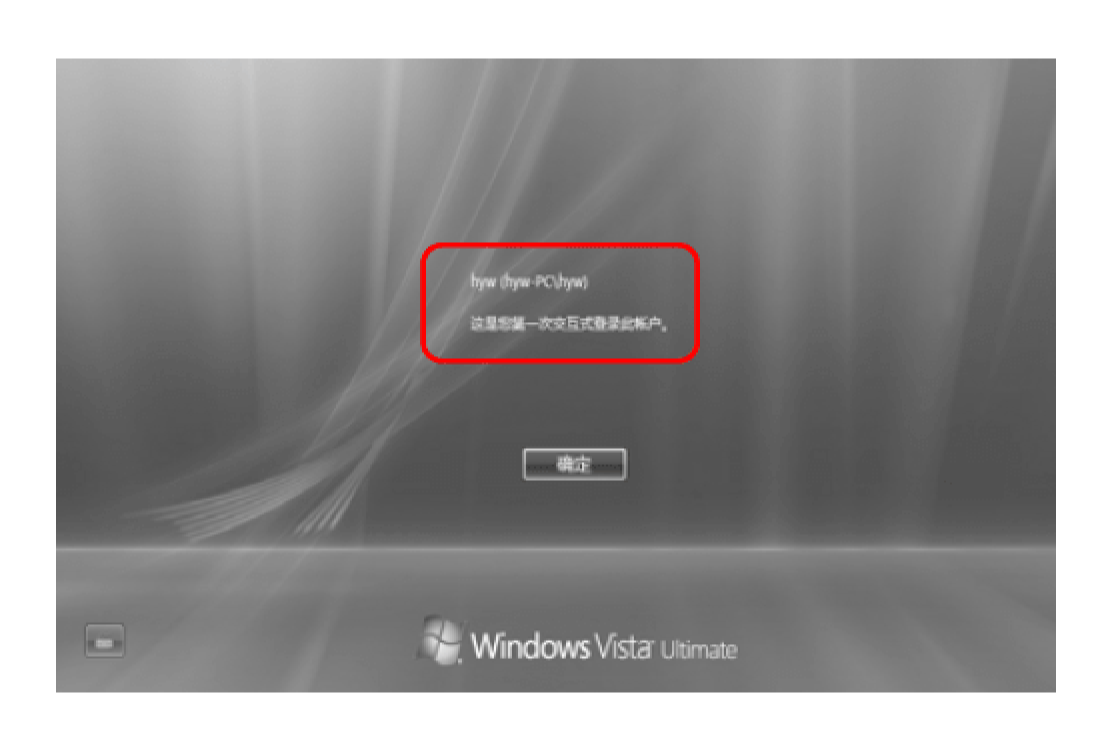
用户设置了此功能后，系统会在登录界面显示上一次登录成功或失败的时间，可以检查是否有非法登录的记录。

❶ 打开组策略对象编辑器，选择“计算机配置”→“管理模块”→“Windows 组件”→“Windows 登录选项”命令。

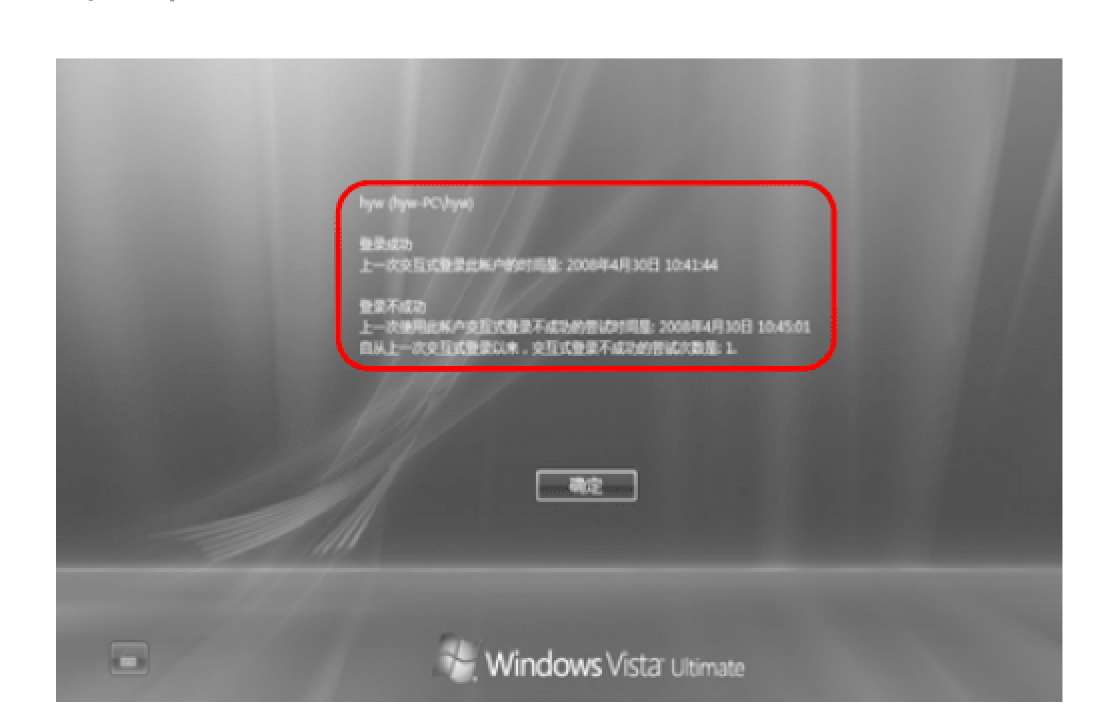




❺ 重新启动电脑。



❻ 再次重新启动电脑，登录失败一次后再进入系统，发现界面上显示了一次登录成功的记录和一次登录失败的记录。





举 一 反 三

如果要撤销此功能，只要将“在用户登录期间显示有关以前的登录信息”功能禁用即可。

技巧193 禁用来宾账户防范黑客攻击

黑客能通过提升来宾账户权限来达到入侵的目的。为此，可以禁用来宾账户来防止黑客入侵系统。

❶ 选择“开始”→“控制面板”命令，双击“用户帐户”图标。









专 家 坐 堂

来宾账户是为电脑上没有永久账户的用户使用的账户。允许用户使用电脑，但没有访问个人文件的权限，且没有安装软件或硬件、更改设置或创建密码的权限。

技巧194 两招禁用 Vista 的用户账户控制

Windows Vista 无论做什么操作，经常会弹出一个“用户帐户控制”对话框。这是微软新增的安全策略，对于有些用户来说，可能会觉得 Windows Vista 的新功能“用户帐户控制”不便。这一功能可以根据需要将其禁止。

(1) 通过控制面板禁止

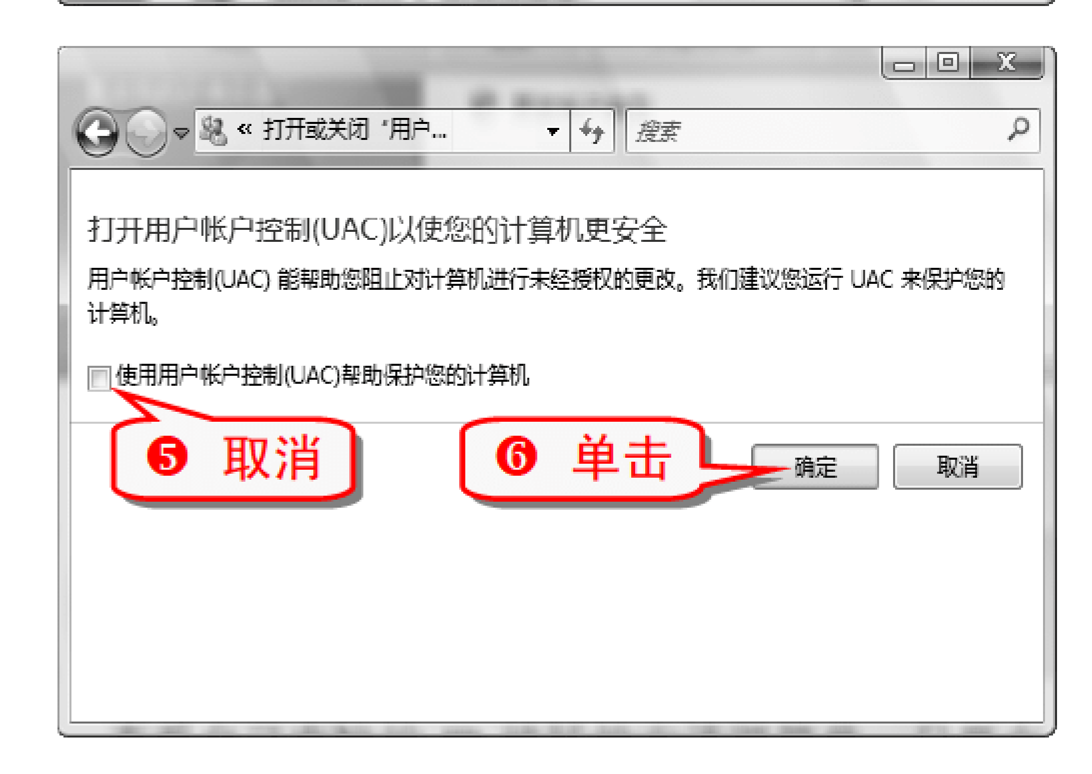
❶ 选择“开始”→“控制面板”命令。





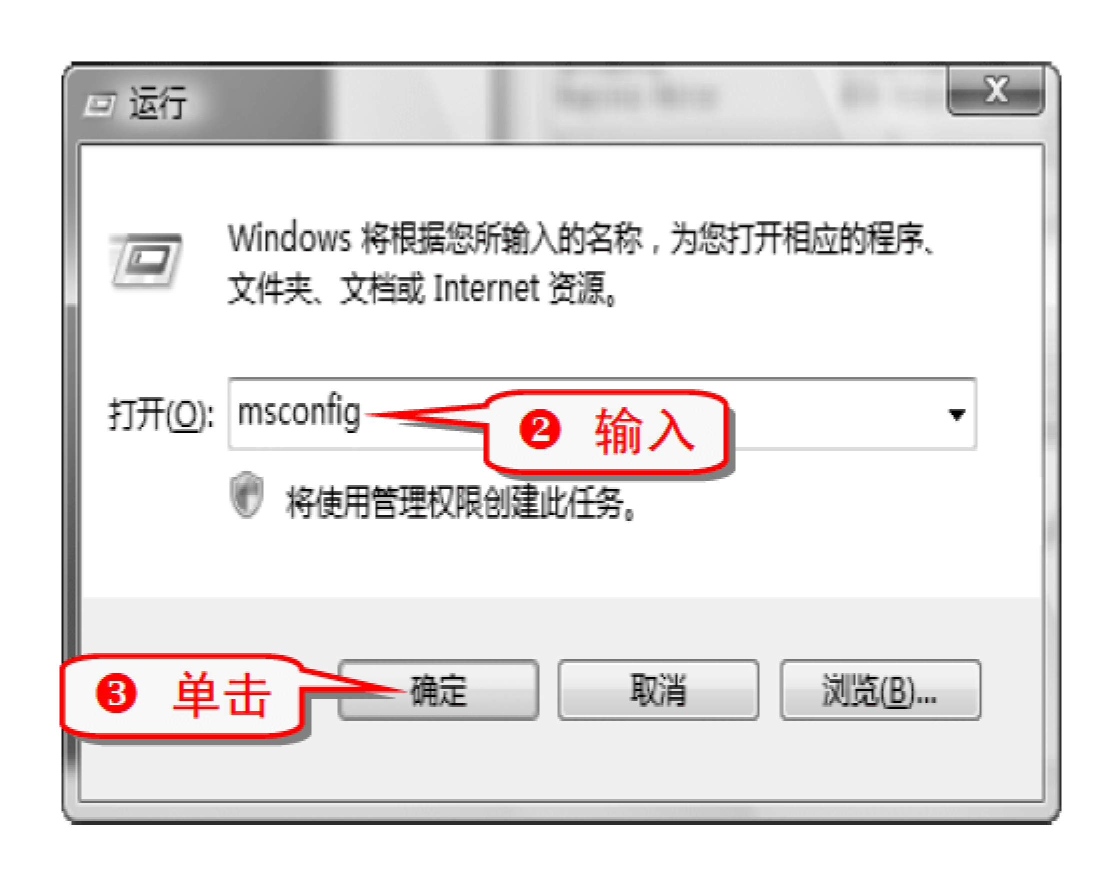


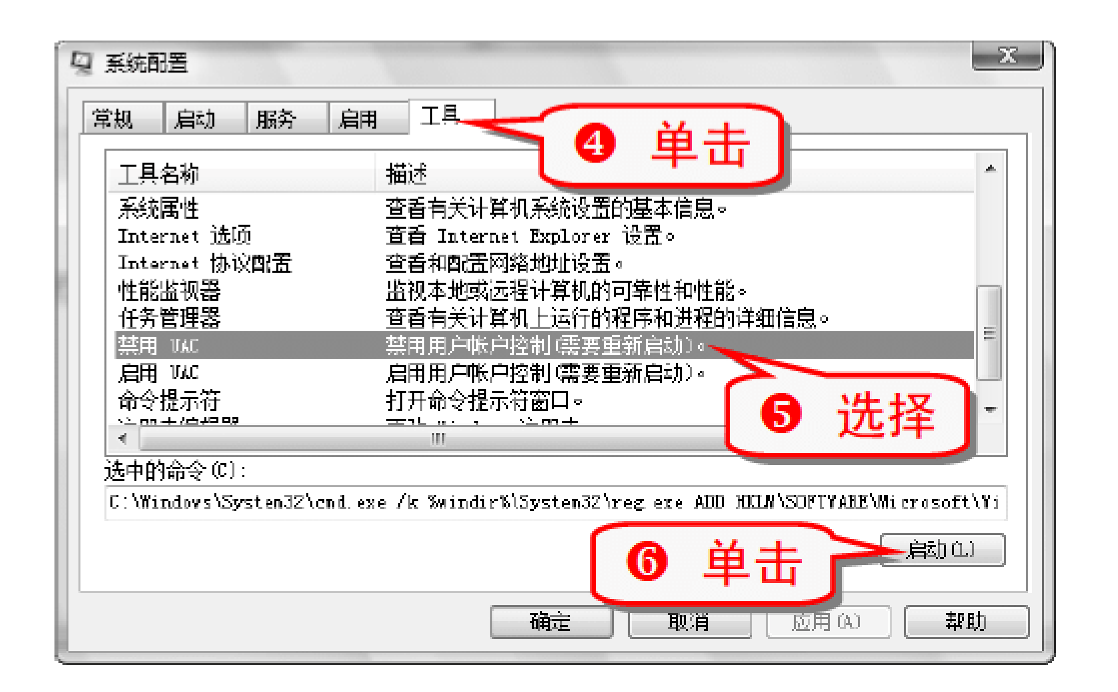




(2) 通过系统配置快速禁止

❶ 按下 ⊞ +R 组合键，打开“运行”对话框。





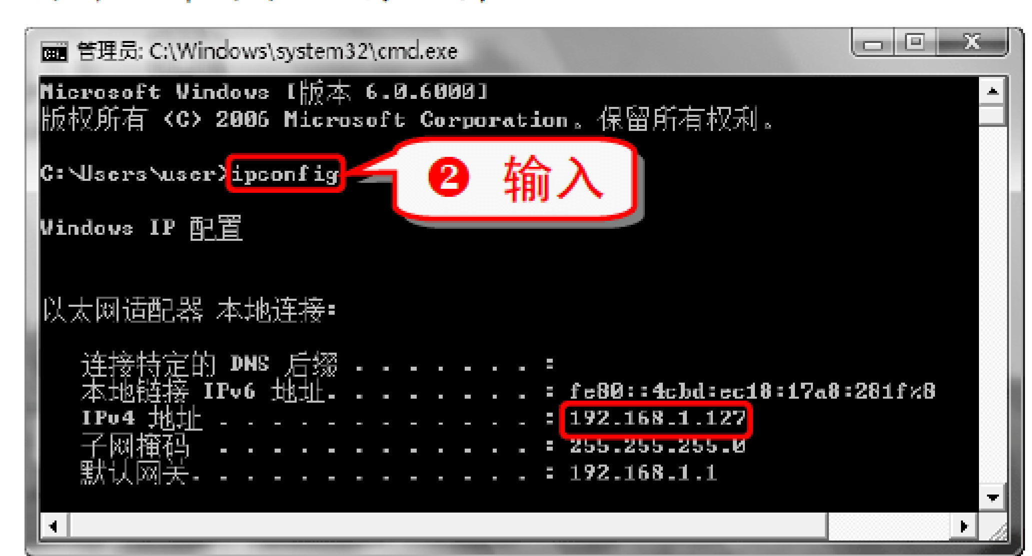
注　意　事　项

禁用用户账户控制以后，必须重新启动电脑才会生效。

技巧195　巧查 IP 地址

查看电脑 IP 地址的方法很简单，只要在“命令提示符”窗口中输入一个命令就可以了。

❶ 打开“运行”对话框，输入 cmd 命令，按下 Enter 键，打开“命令提示符”窗口。

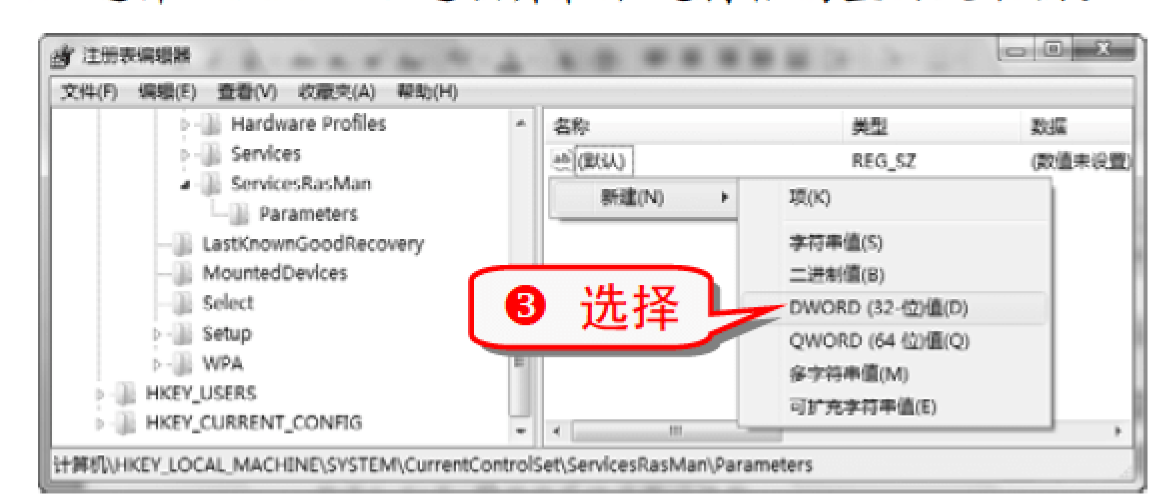


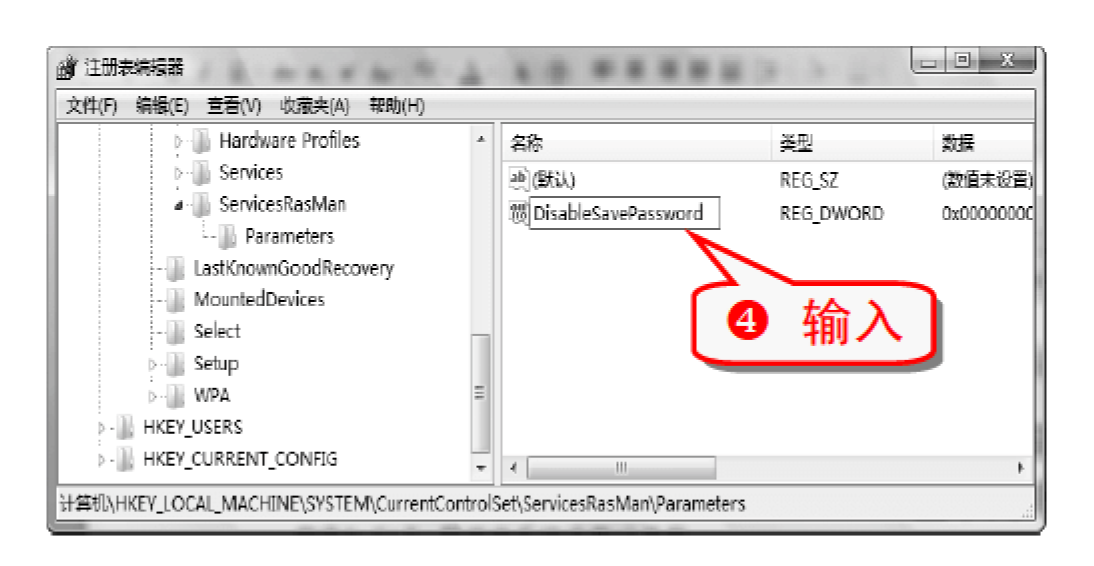
技巧196　保护拨号网络密码的安全

使用拨号网络时，一些系统会自动将网络口令和密码记录在电脑上，很容易被密码查看器找出密码。通过修改注册表，可以很好地保护拨号网络密码的安全。

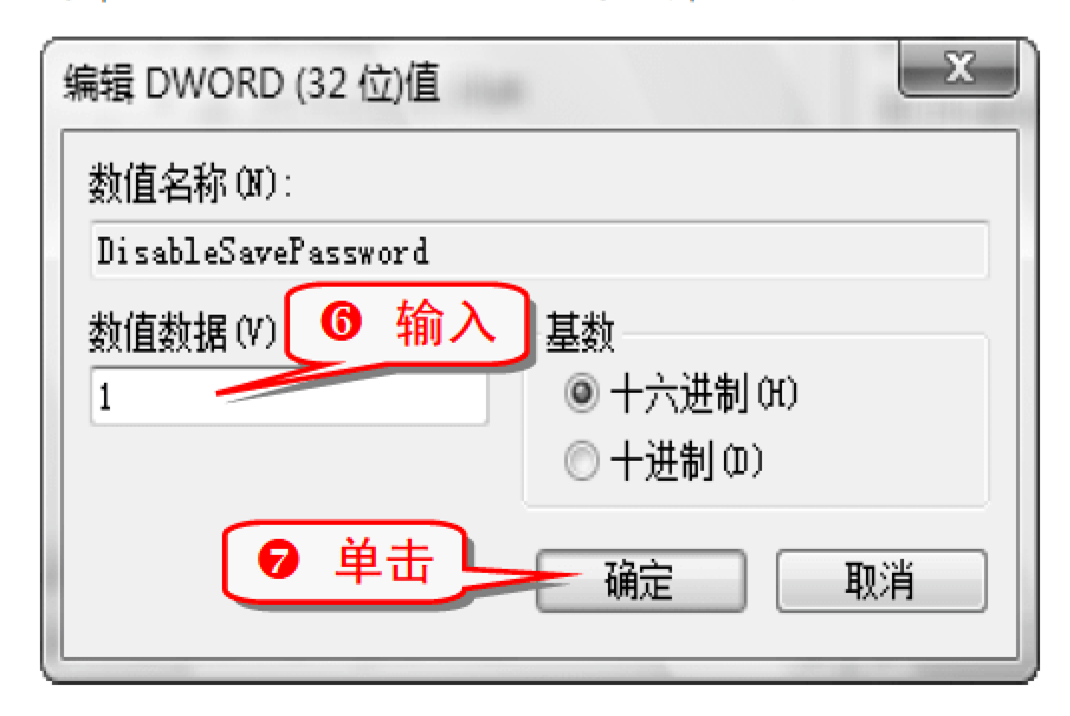
❶ 打开注册表编辑器，展开 HKEY_LOCA L_MACHINE\SYSTEM\CurrentControlSet\ServicesRasMan\Parameters 分支。

❷ 选择 Parameters 选项并在右边窗格的空白处右击。





❺ 选中 DisablePassword 选项并双击。

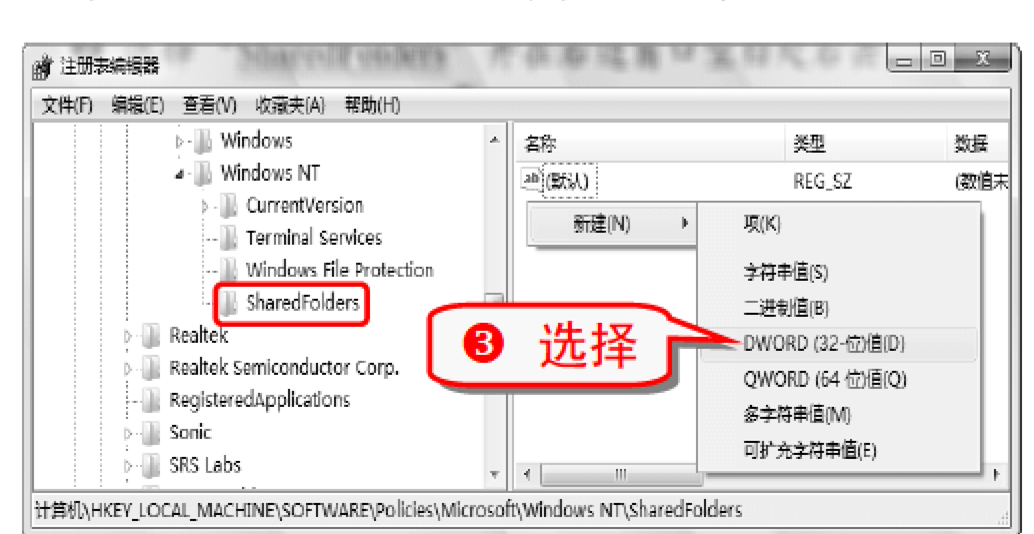


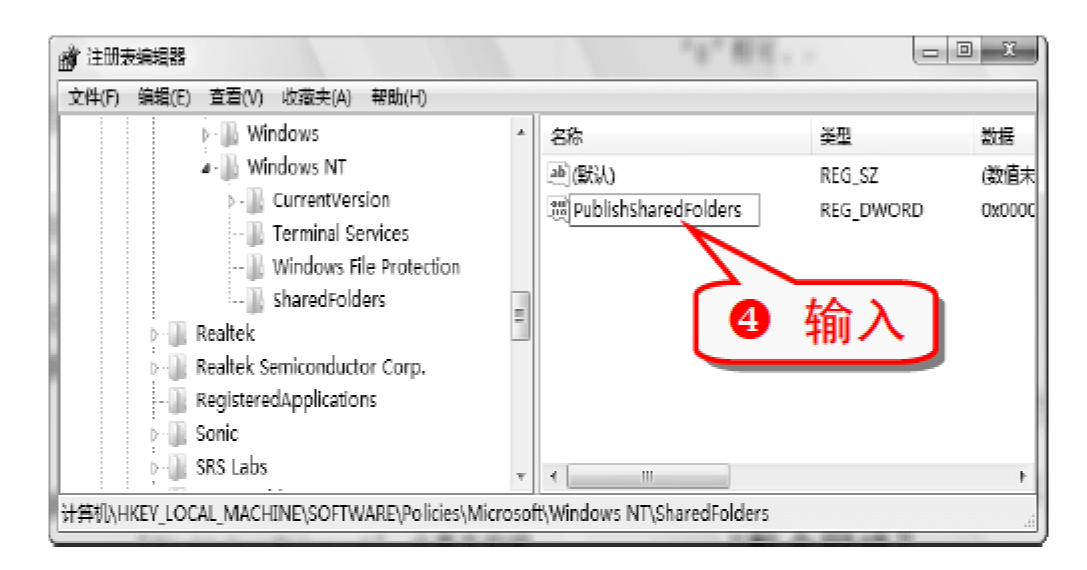
技巧197 禁止发布共享文件夹

发布共享文件夹，可能会泄露重要信息。可以通过修改注册表来禁止发布共享文件夹。

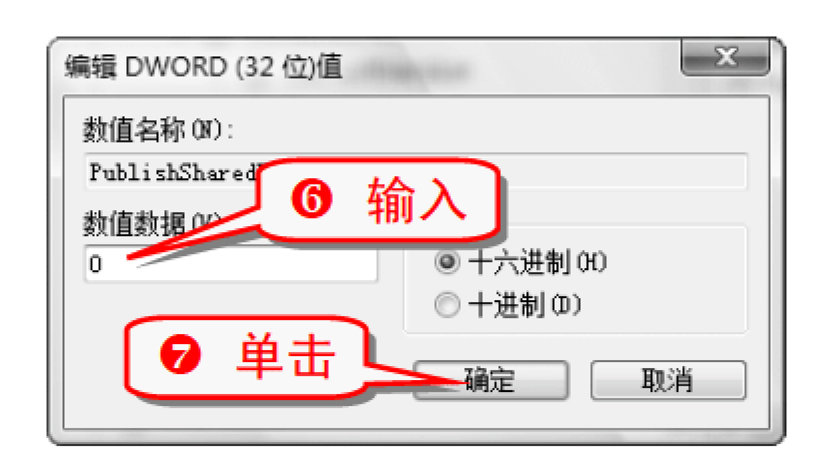
❶ 打开注册表编辑器，展开 HKEY_LOCA L_MACHINE\SOFTWARE\Policies\Microsoft\WindowsNT\SharedFolders 分支。

❷ 选择 SharedFolders 选项并在右边窗格空白处右击。





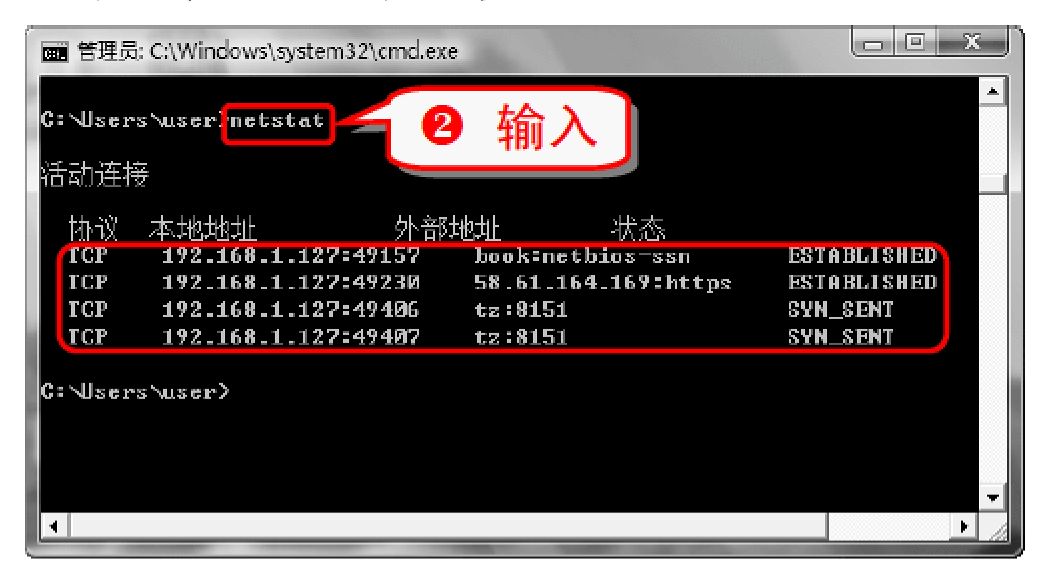
❺ 选中 PublishSharedFolders 选项并双击。



技巧198 查看与当前电脑相连的电脑的IP 地址

要查看与当前电脑相连的电脑的 IP 地址，也只需要一个 DOS 命令。

❶ 打开“运行”对话框，输入 cmd 命令，按下 Enter 键，打开“命令提示符”窗口。



技巧199 查看网络上电脑的 IP 地址

查看网络上电脑的 IP 地址的方法有很多，下面介绍 3 种常用的方法。

(1) 使用 Ping 命令查看

Ping 命令是一个 16 位的命令行程序，下面介绍如何通过 Ping 命令查看 www.baidu.com 网站主机的 IP 地址。

❶ 打开“运行”对话框，输入 cmd 命令，按下 Enter 键，打开“命令提示符”窗口。

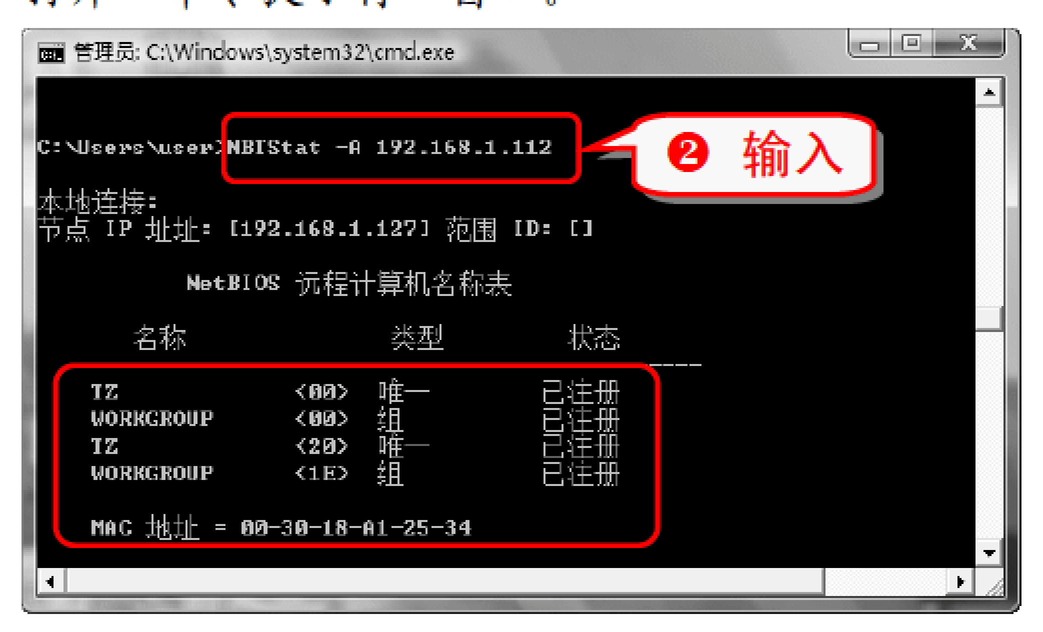


(2) 使用 NBTStat 命令查看

相较于使用 Ping 命令使用 NBTStat 命令获得的信息更多。



❶ 打开“运行”对话框，输入 cmd 命令，按下 Enter 键，打开“命令提示符”窗口。



(3) 使用 route print 命令

使用 route print 命令可以查看自己的路由表信息。

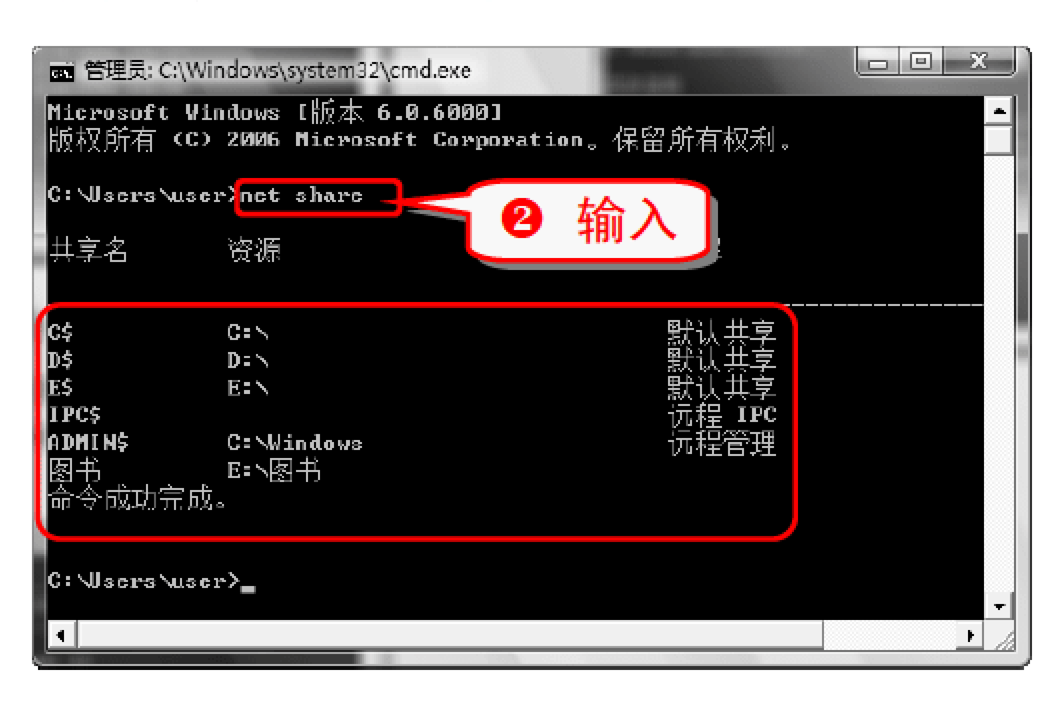
❶ 打开“运行”对话框，输入 cmd 命令，按下 Enter 键，打开“命令提示符”窗口。



技巧200　用 net share 查看本地共享资源

使用 net share 命令可以查看当前电脑开放了多少共享资源。

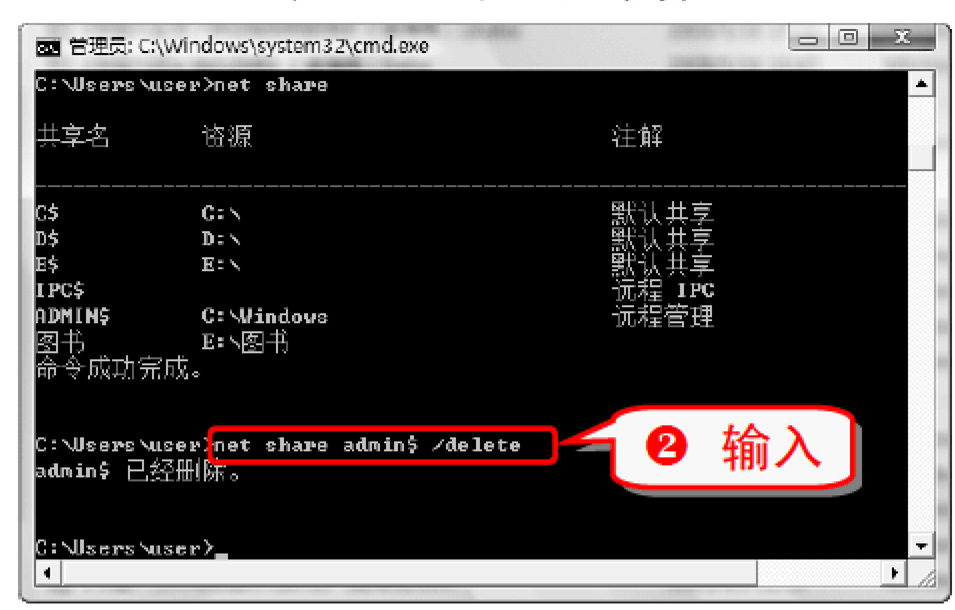
❶ 打开“运行”对话框，输入 cmd 命令，按下 Enter 键，打开“命令提示符”窗口。

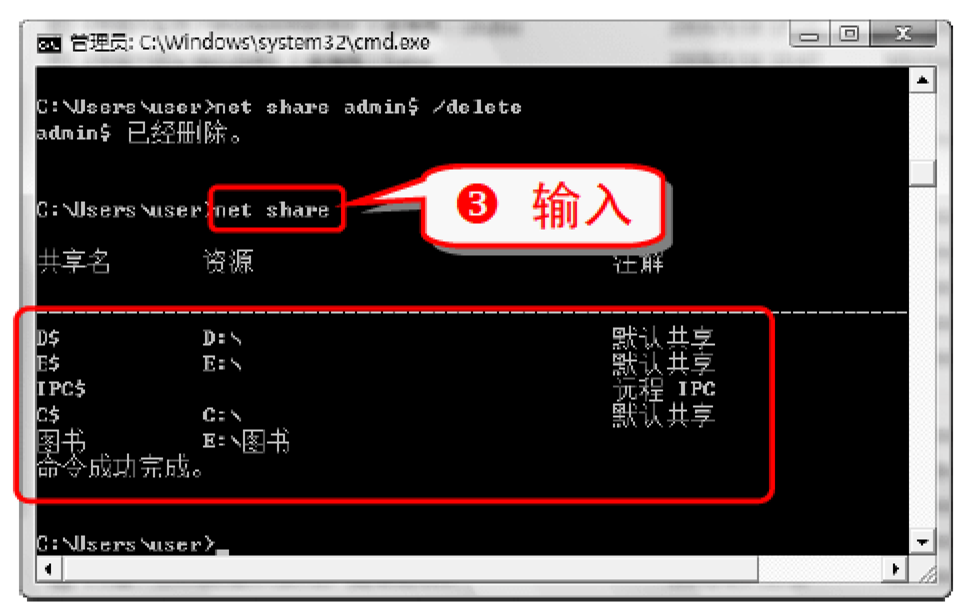


技巧201　手动删除本地共享资源

对于一些不必要的共享资源，应将其删除，而这一过程用一个 DOS 命令就可以实现。

❶ 使用 net share 命令列出本地共享资源。





专　家　坐　堂

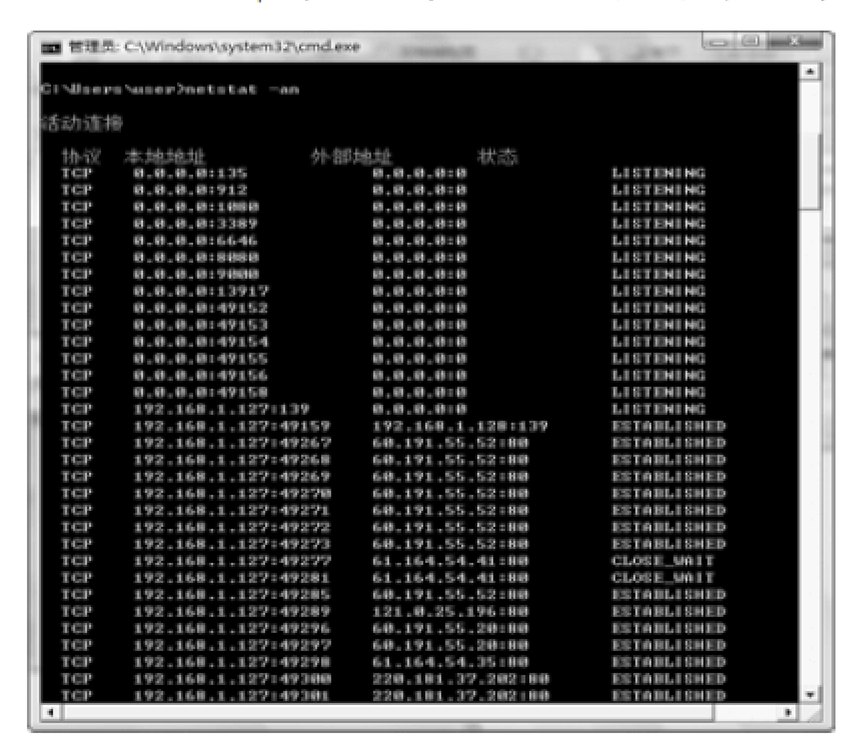
如果下次重新启动电脑后发现被删除的共享又出现了，那可能是电脑中病毒了。

技巧202　查看本地所有开放端口

当前最为常见的木马通常是基于 TCP/UDP 协议进行通信的，可以利用查看本机开放端口的方法来检查是否被中了木马或其他 hacker 程序。利用系统自带的命令可以快速查看电脑开放了哪些端口。

❶ 打开“运行”对话框，输入 cmd 命令，按下 Enter 键，打开“命令提示符”窗口。

❷ 输入 netstat -an 命令，按下 Enter 键。结果如下图所示。

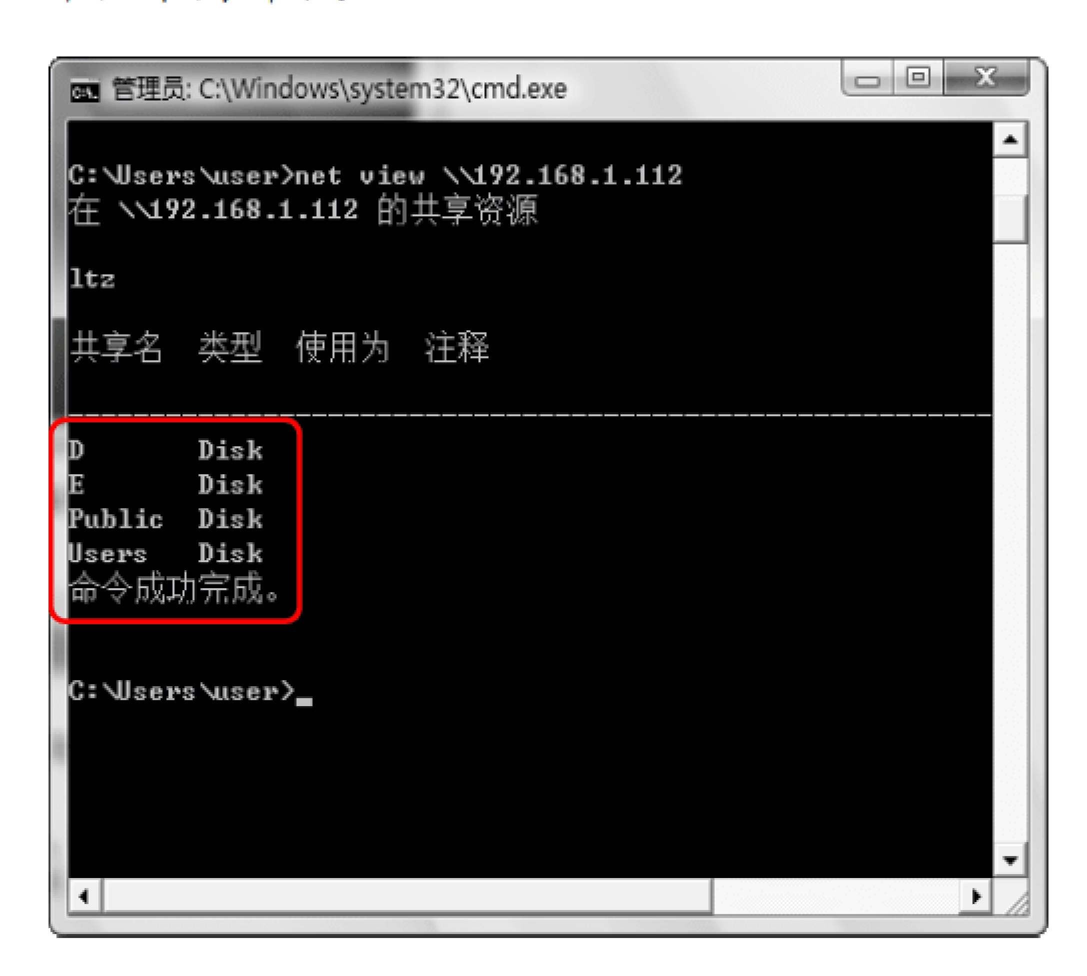


技巧203 查看局域网中指定电脑的共享资源

在同一个局域网中，只要知道对方的 IP 地址就可以利用系统命令查看对方的共享资源。

❶ 打开“运行”对话框，输入 cmd 命令，按下 Enter 键，打开“命令提示符”窗口。

❷ 输入 net view \\192.168.1.112 命令，按下 Enter 键。结果如下图所示。



技巧204 查看电脑的详细网络配置

系统自带的 ipconfig/all 命令能查看当前电脑的详细网络配置，包括 MAC 地址。

❶ 打开“运行”对话框，输入 cmd 命令，按下 Enter 键，打开“命令提示符”窗口。

❷ 输入 ipconfig/all 命令，按下 Enter 键。结果如下图所示。

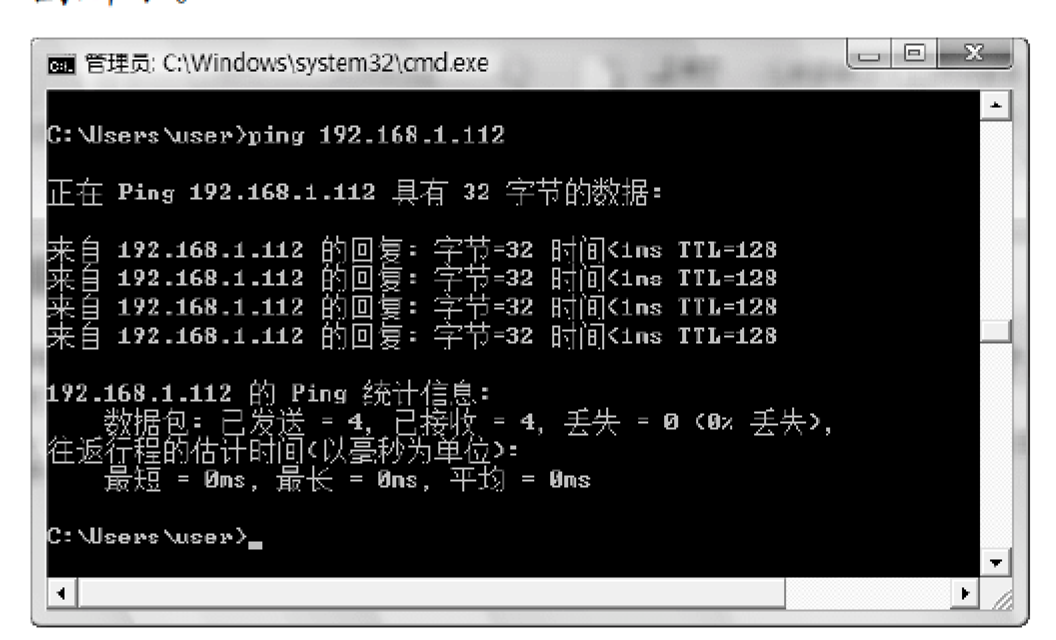


技巧205 测试物理网络命令

利用系统自带的 Ping 命令，可以查看某个 IP 地址是否是活跃的，也就是拥有该 IP 地址的电脑是否处于开机状态。

❶ 打开“运行”对话框，输入 cmd 命令，按下 Enter 键，打开“命令提示符”窗口。

❷ 输入 ping 192.168.1.1 命令，按下 Enter 键。结果如下图所示。





专 家 坐 堂

可以用 ping 命令查看当前电脑是否连在路由器上，或是检测某电脑的 IP 地址是否处于活跃状态。

数据包没有丢失，证明 ping 的电脑处于开机状态，如果数据包 100%丢失，证明电脑处于关机或断网状态。

技巧206 探测 ARP 绑定列表

用 arp -a 命令探测 ARP 绑定(动态和静态)列表，可以显示所有连接到当前电脑的 IP 地址和 MAC 地址。

❶ 打开“运行”对话框，输入 cmd 命令，按下 Enter 键，打开“命令提示符”窗口。

❷ 输入 arp-a 命令，按下 Enter 键。结果如下图所示。

```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.0.6000]
版权所有 (C) 2006 Microsoft Corporation。保留所有权利。

C:\Users\user>arp -a

接口: 192.168.1.127 --- 0x8
  Internet 地址         物理地址              类型
  192.168.1.1           00-0e-a0-00-44-b7     动态
  192.168.1.102         00-30-18-a1-22-2a     动态
  192.168.1.105         00-30-18-a3-5d-b7     动态
  192.168.1.106         00-30-18-a1-27-ea     动态
  192.168.1.108         00-30-18-a1-1f-15     动态
  192.168.1.109         00-30-18-a1-29-e7     动态
  192.168.1.112         00-30-18-a1-25-34     动态
  192.168.1.128         00-15-f2-bd-d2-68     动态
  192.168.1.129         00-0a-eb-40-2c-eb     动态
  192.168.1.255         ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     静态
  224.0.0.22            01-00-5e-00-00-16     静态

C:\Users\user>_
```

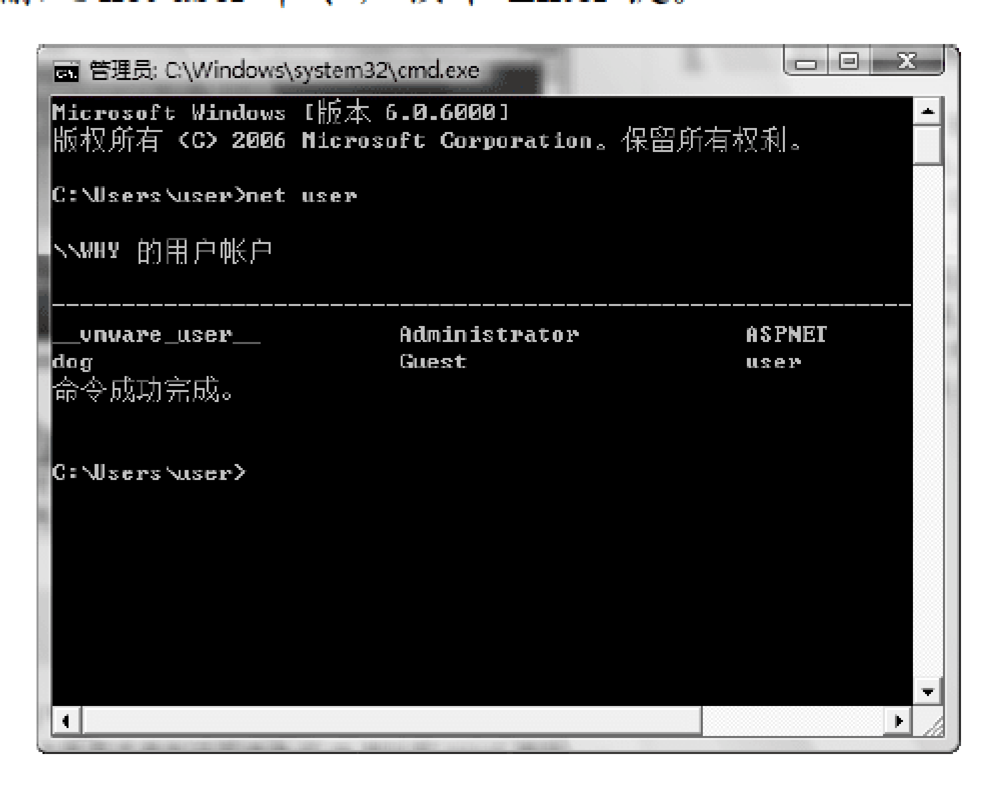


技巧207　查看当前电脑的用户账号列表

使用 net user 命令查看当前电脑上的账户列表，可以检查是否有非法添加的具有管理员级别的账户。

❶ 打开“运行”对话框，输入 cmd 命令，按下 Enter 键，打开“命令提示符”窗口。

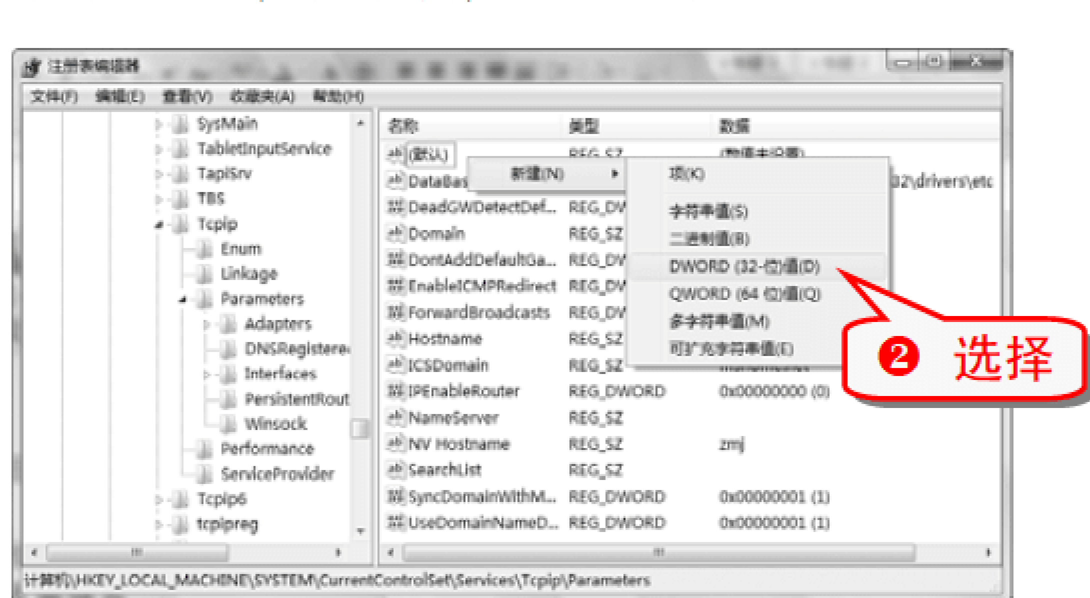
❷ 输入 net user 命令，按下 Enter 键。

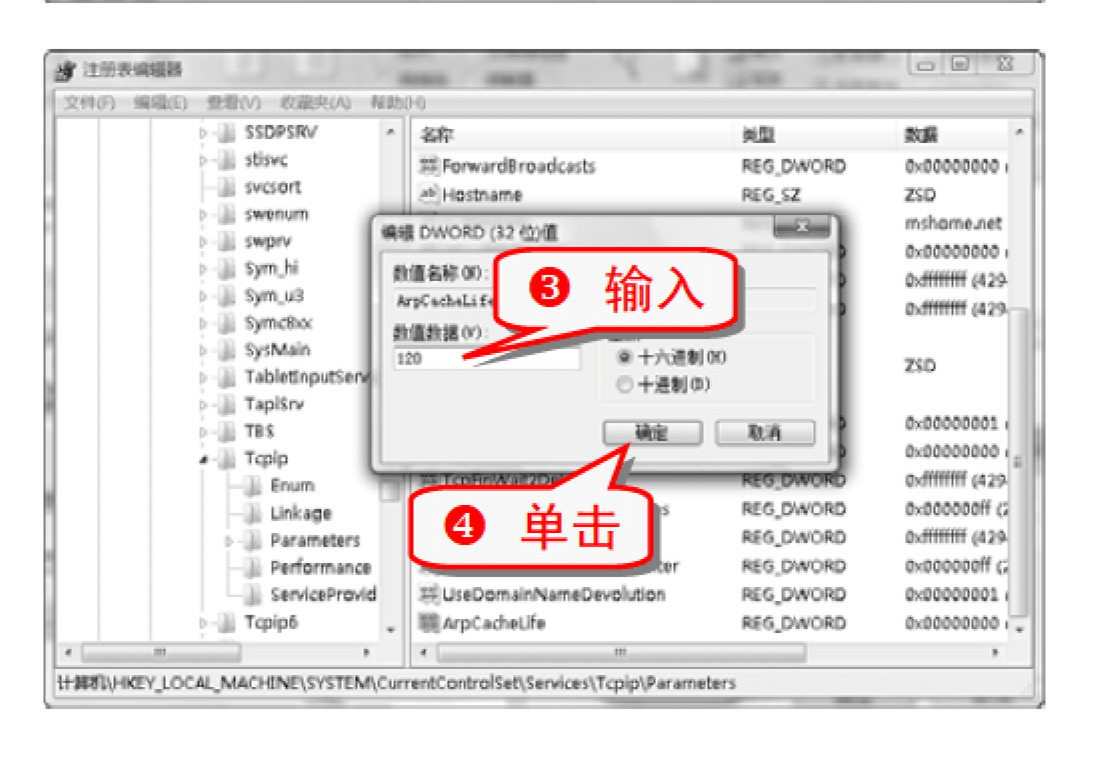


技巧208　设置 ARP 缓存老化时间

地址解析协议(Address Resolution Protocol)，可以把 MAC 地址解析成 IP 地址，设置 ARP 缓存老化时间，能够防止 ARP 被欺骗。

❶ 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 分支，然后在右边的窗格空白区右击。





技巧209　检查重要文件扩展名

EXE、COM、PIF、BAT、SCR、TXT、INI、INF 以及 CHM，这些系统重要文件的扩展名的值(打开方式)是不变的。很多木马程序会修改其打开方式，当运行该类型扩展名的文件时，木马程序也会一起启动。有很多工具可以查看这些文件扩展名是否被修改，如 System Repair Engineer。

(1) 启动项目管理

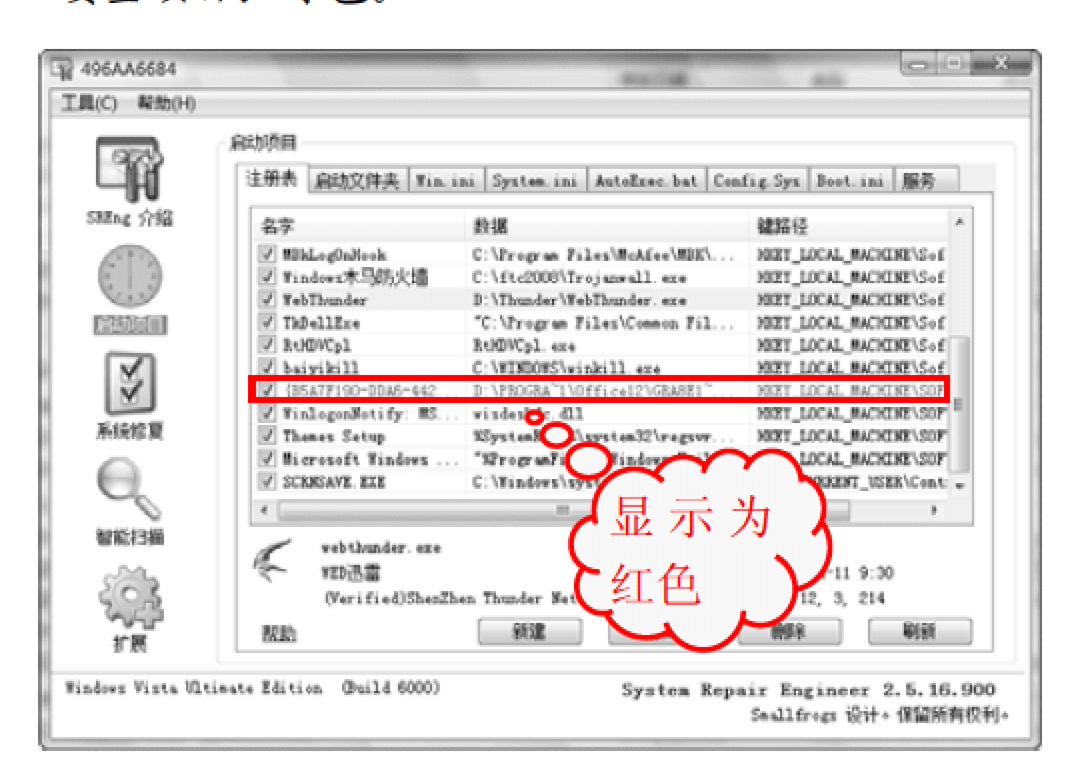
System Repair Engineer 的启动项目由 8 个部分组成：注册表类、启动文件夹类、配置文件类(WIN.INI、SYSTEM.INI、AUTOEXEC.BAT、CONFIG.SYS)、BOOT.INI 文件类以及服务类。

注册表类的启动项目由十多个注册表键值所含数据组成。打开注册表类启动项目窗口以后，System Repair Engineer 会检测系统里面所有的被支持的能够随机启动的注册表键值，然后把相关结果显示出来。

如果 System Repair Engineer 发现默认的键值被修改成非默认值，且这个键值经常被病毒修改，那么会弹出一个警告提示提醒用户注意。

当 System Repair Engineer 发现一个可疑的项目，会以颜色高亮显示。System Repair Engineer 的颜色方案如下。

- 高危项目：红色。
- 未知安全等级项目：蓝色。
- 安全项目：绿色。

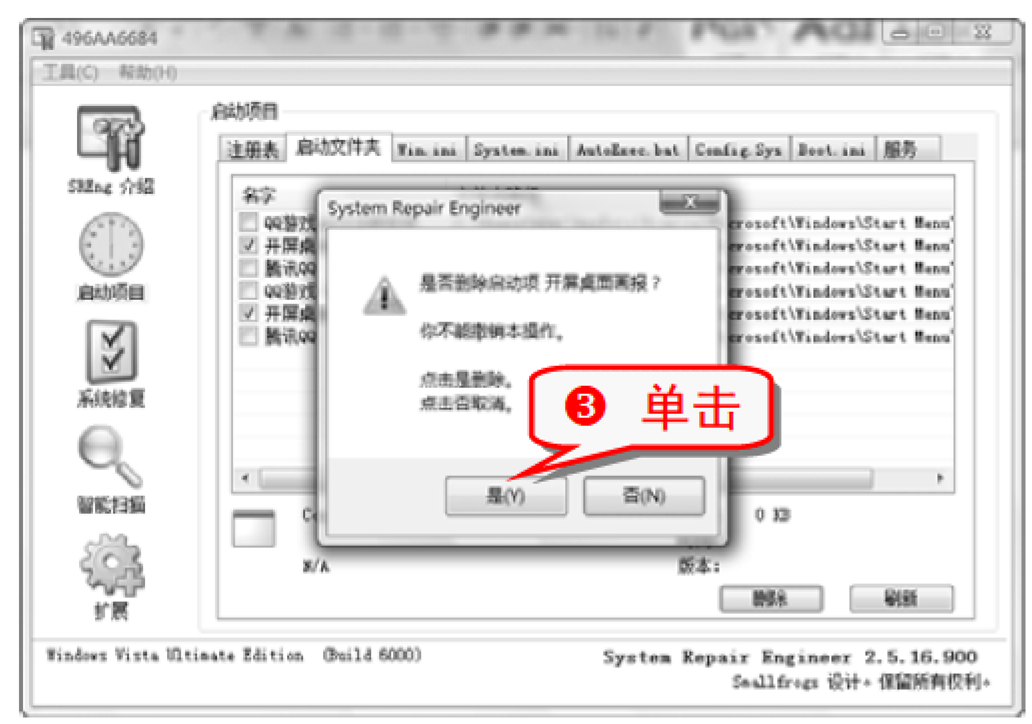


专　家　坐　堂

根据 Windows 的设计，启动文件夹分为公用启动文件夹和私有启动文件夹。公用启动文件夹里面的启动快捷方式对所有用户均有效，而私有启动文件夹里面的快捷方式仅对当前用户有效。System Repair Engineer 能够同时支持公用启动文件夹和私有启动文件夹的信息获取并将相关信息显示出来。

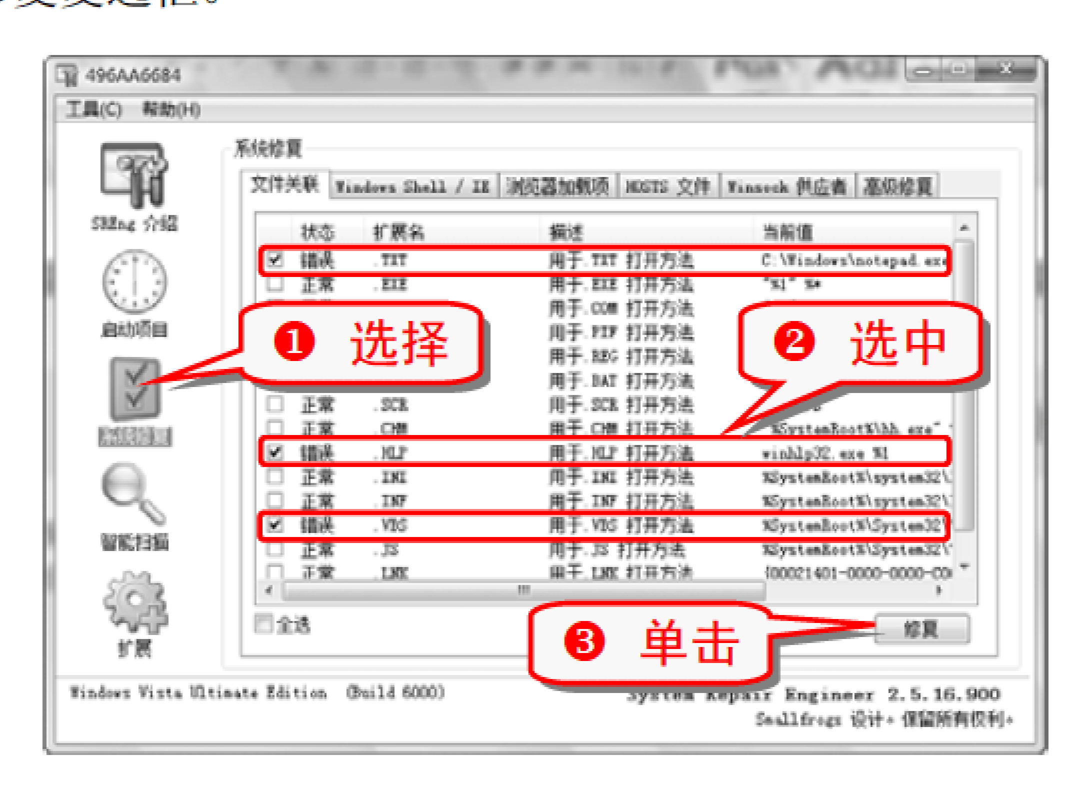
管理启动文件夹的步骤如下。





(2) 系统修复

文件关联部分在原有基础上增加了自动侦测功能，对于非默认文件关联值会显示一个错误标识并且自动选中修复复选框。

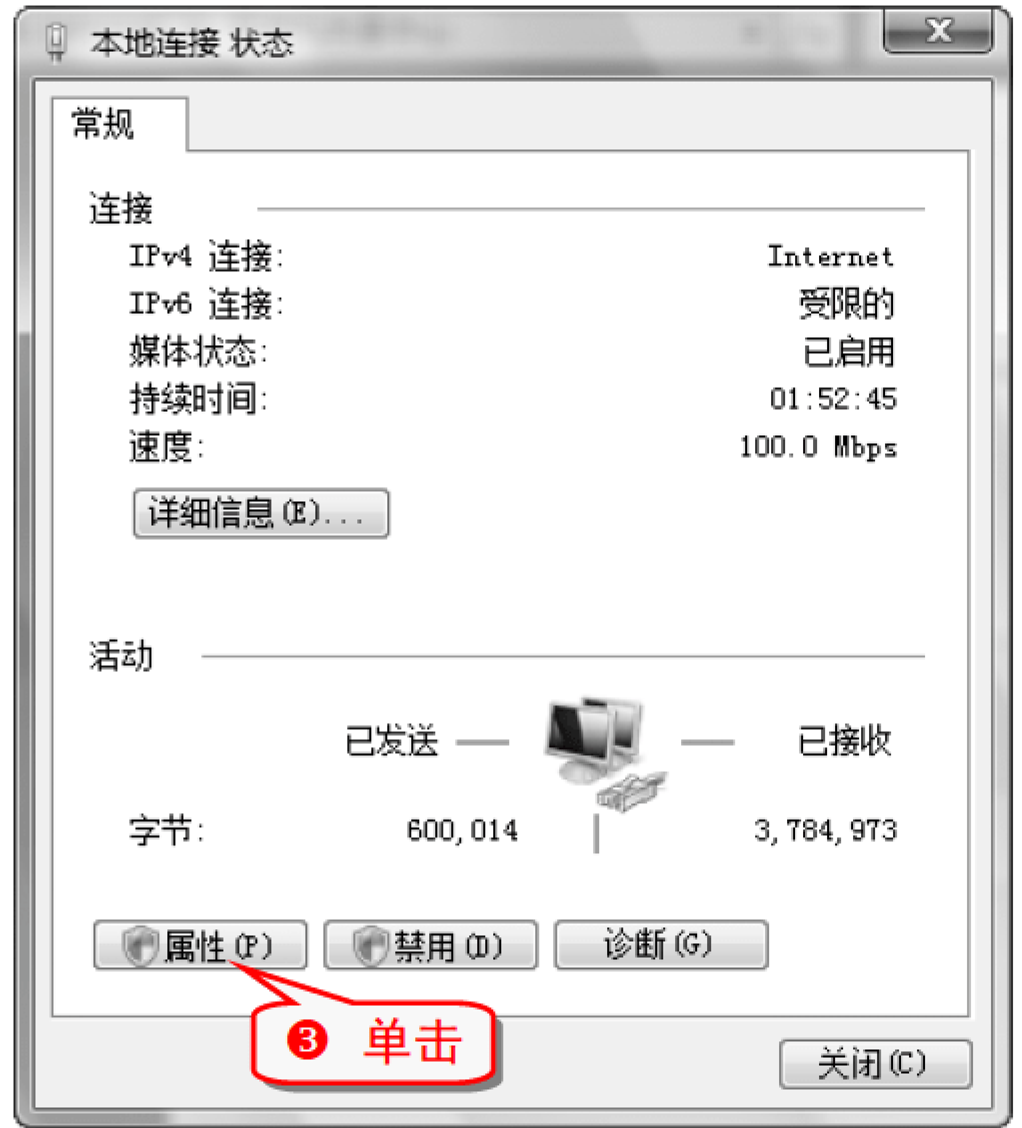


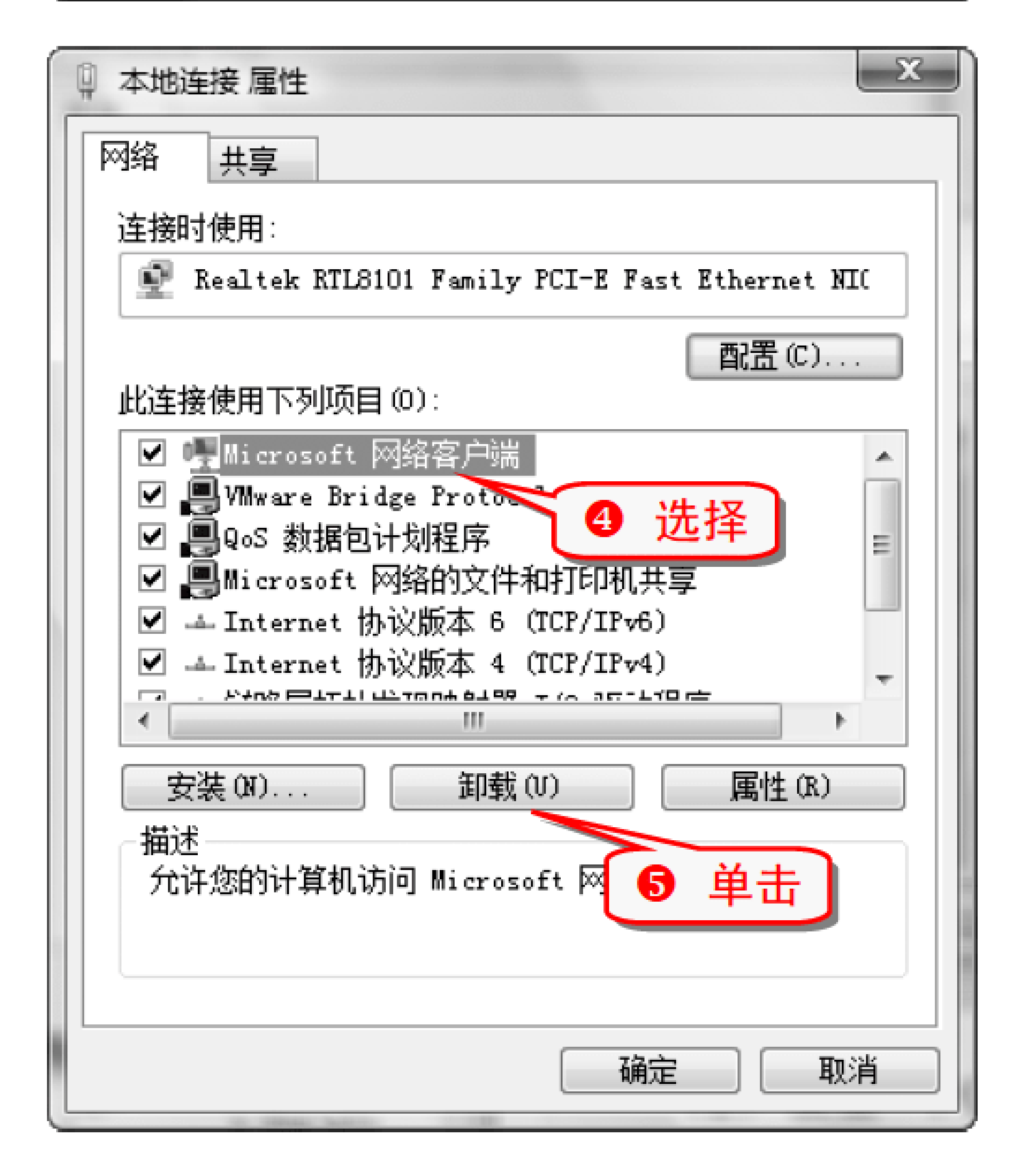
技巧210 关闭多余的协议

对于一般的个人用户而言，用到的只有TCP/IP协议，可以关闭其他多余的协议。

❶ 右击“网络”图标，在弹出的快捷菜单中选择“属性”命令，打开“网络和共享中心”窗口。







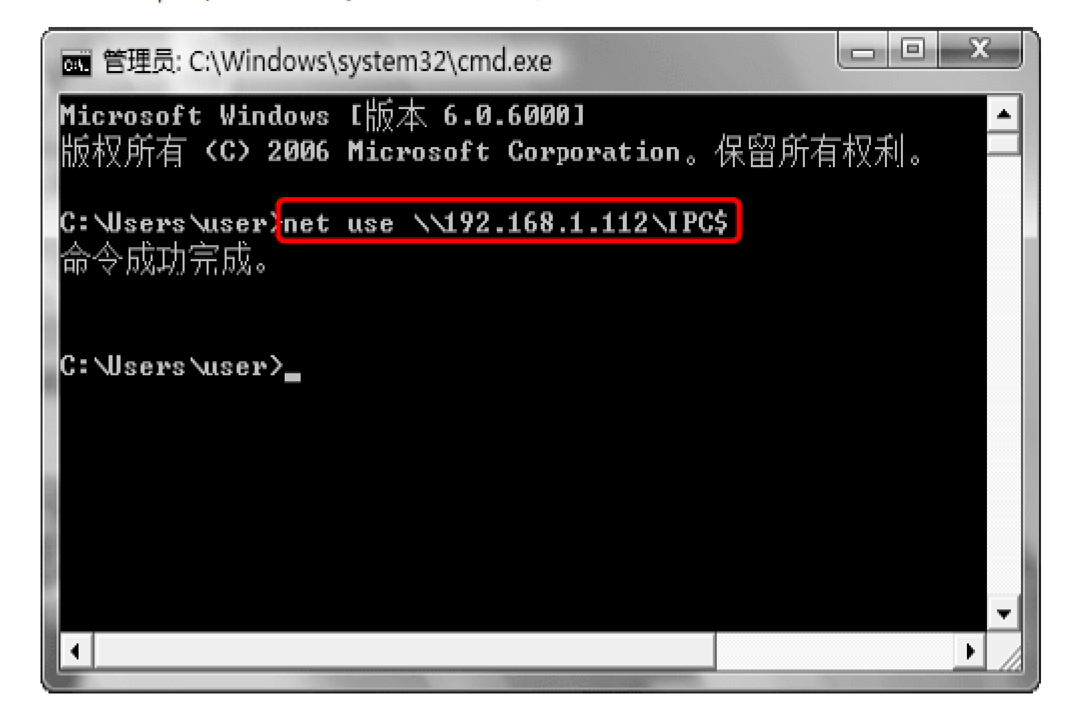


技巧211　IPC$入侵的 4 种方式

IPC$(Internet Process Connection)是共享“命名管道”的资源，是为了让进程间能通信而开放的命名管道，在提供可信任的用户名和密码的前提下，连接双方可以建立的安全管道并通过该管道进行数据交换。

(1) 建立空连接

❶ 打开“命令提示符”窗口，输入 net use \\192.168.1.112\IPC$命令，按下 Enter 键。



❷ 系统提示“命令成功完成”，空连接已经建立完毕。

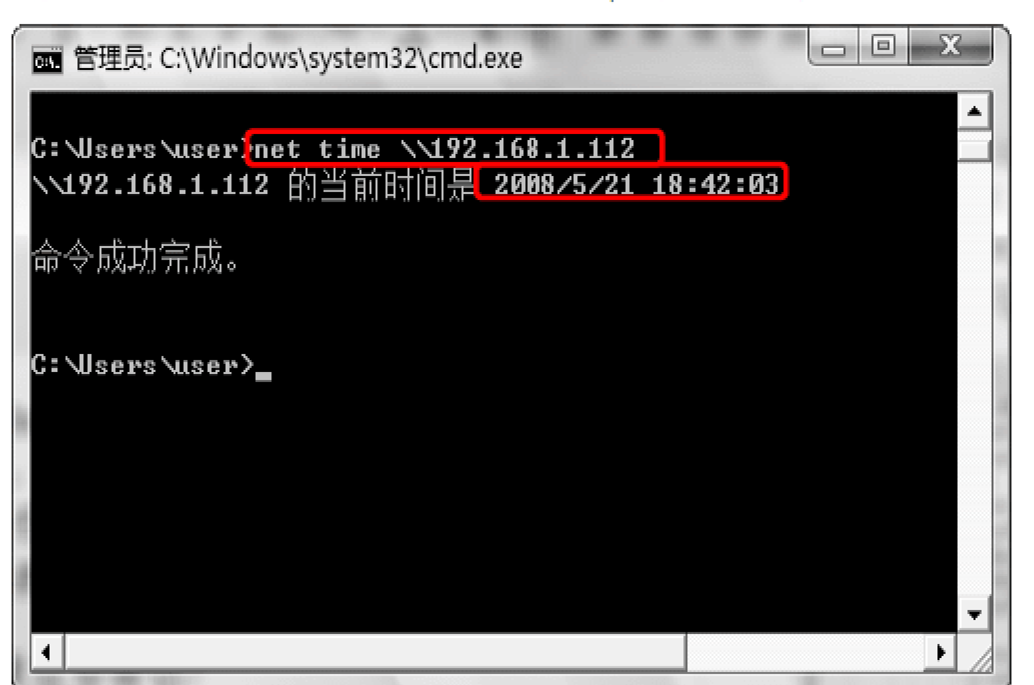
举 一 反 三



只需要在建立空连接的命令最后添加/del，即删除 IPC$空连接的命令。

(2) 查看远程主机的当前时间

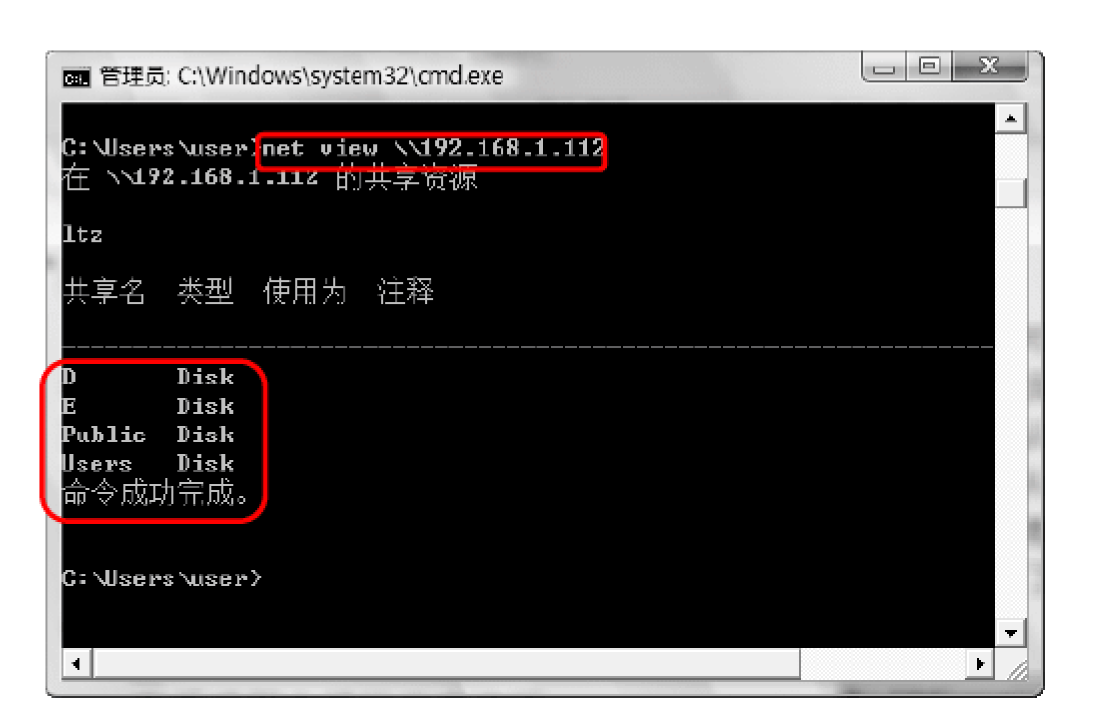
❶ 输入 net time \\192.168.1.112 命令，按下 Enter 键。



❷ 目标主机时间被显示出来，系统提示“命令成功完成”。

(3) 查看远程主机的共享资源

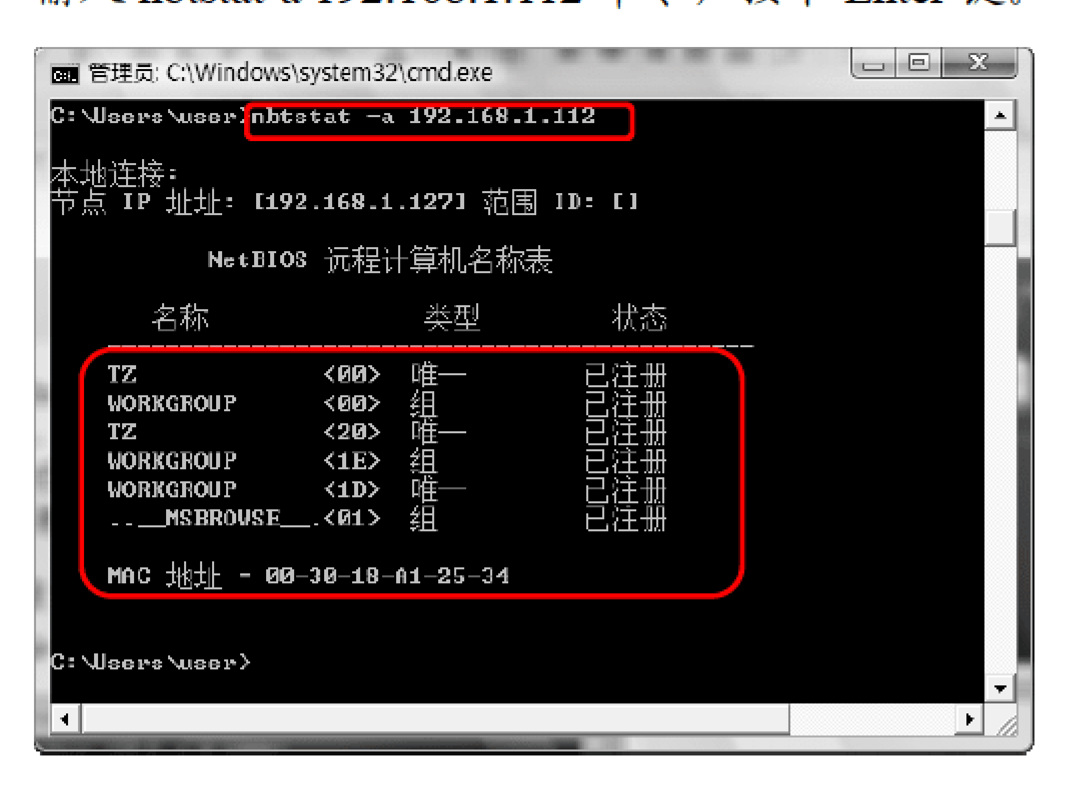
❶ 输入 net view \\192.168.1.112 命令，按下 Enter 键。



❷ 共享的目录被罗列出来，系统提示“命令成功完成”。

(4) 得到远程主机的 NetBIOS 用户名列表

❶ 输入 nbtstat-a 192.168.1.112 命令，按下 Enter 键。



❷ NetBIOS 用户名列表被显示出来。

注 意 事 项

使用空连接可以查询到目标主机很多的信息，不过建立 IPC$连接的操作会在 EventLog 文件中留下记录。

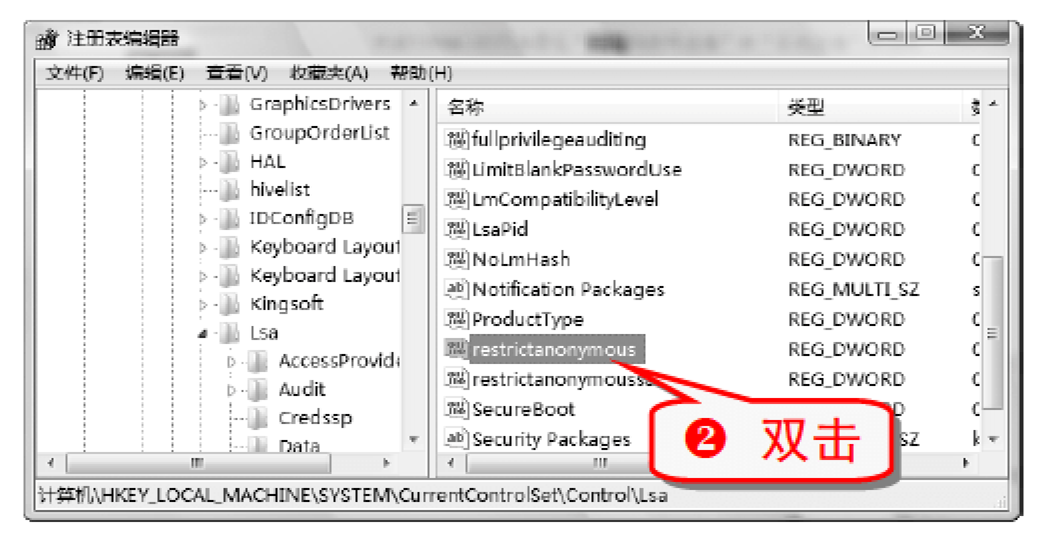
技巧212　四招防范 IPC$入侵

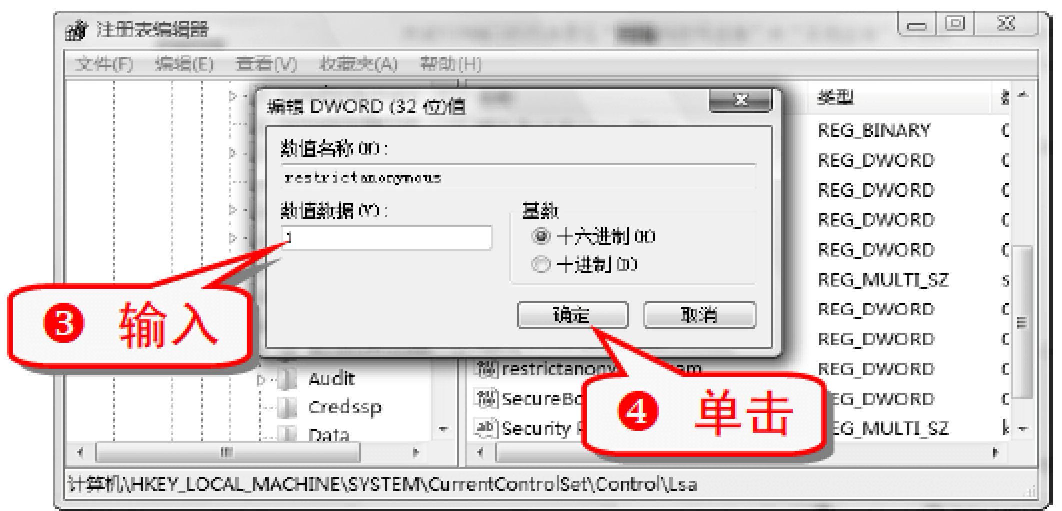
了解到了 IPC$入侵的方法，还应该了解防范的方法，这样才可以防范 IPC$入侵自己的电脑。防范 IPC$入侵的方法主要有以下几种。

(1) 禁止空连接进行枚举

通过禁止空连接进行枚举可以限制通过枚举的方法获得 SAM 账号和共享信息。

❶ 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 分支。

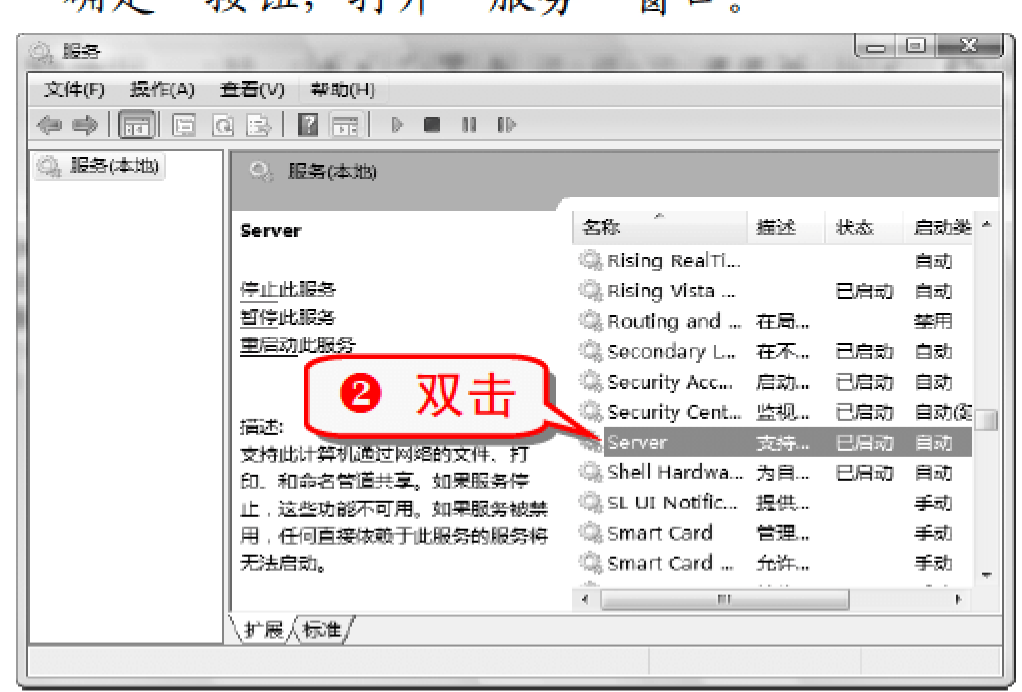


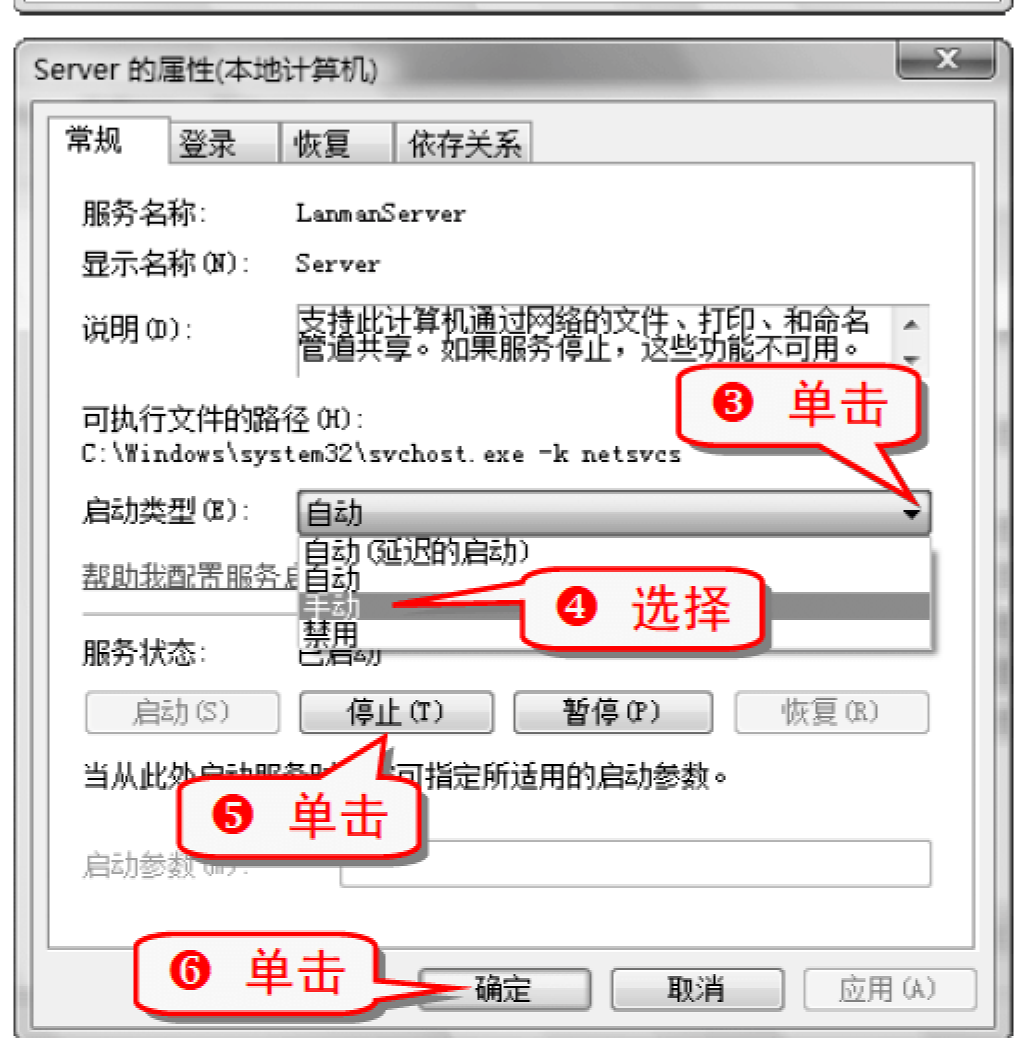


(2) 禁止 IPC$共享

IPC$是系统默认的一种共享资源，在系统中掌控类似IPC$共享资源的是一个名称为 Server 的服务，只要关闭该服务，就可以禁用 IPC$共享。

❶ 打开“运行”对话框，输入 services.msc 命令，单击“确定”按钮，打开“服务”窗口。





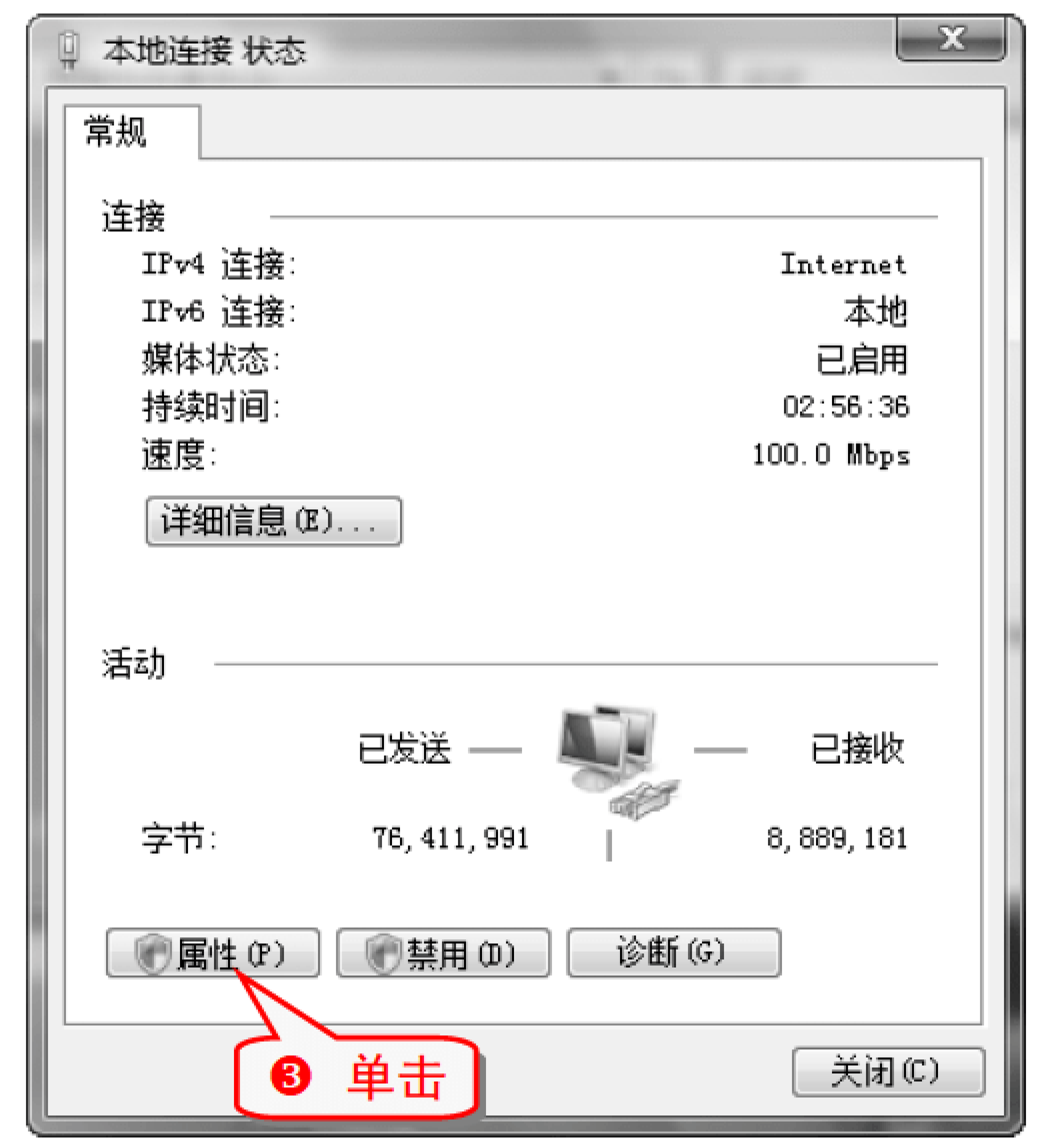
(3) 屏蔽 139 端口

没有 139 端口的支持，是无法建立 IPC$连接的，因此屏蔽 139 端口可以阻止 IPC$入侵。

139 端口可以通过禁止 NBT 来屏蔽。

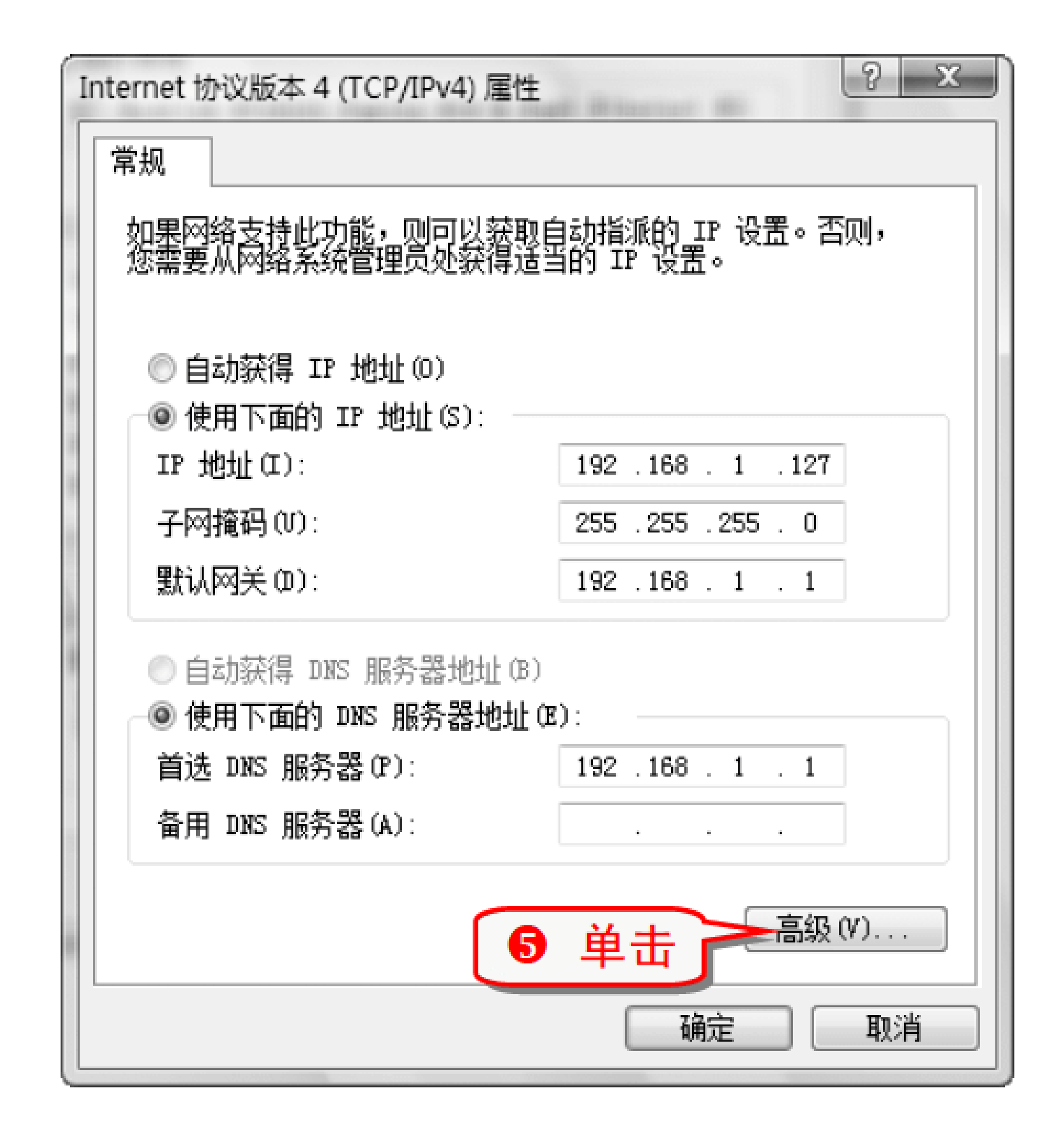
❶ 右击“网络”图标，在弹出的快捷菜单选择“属性”命令。

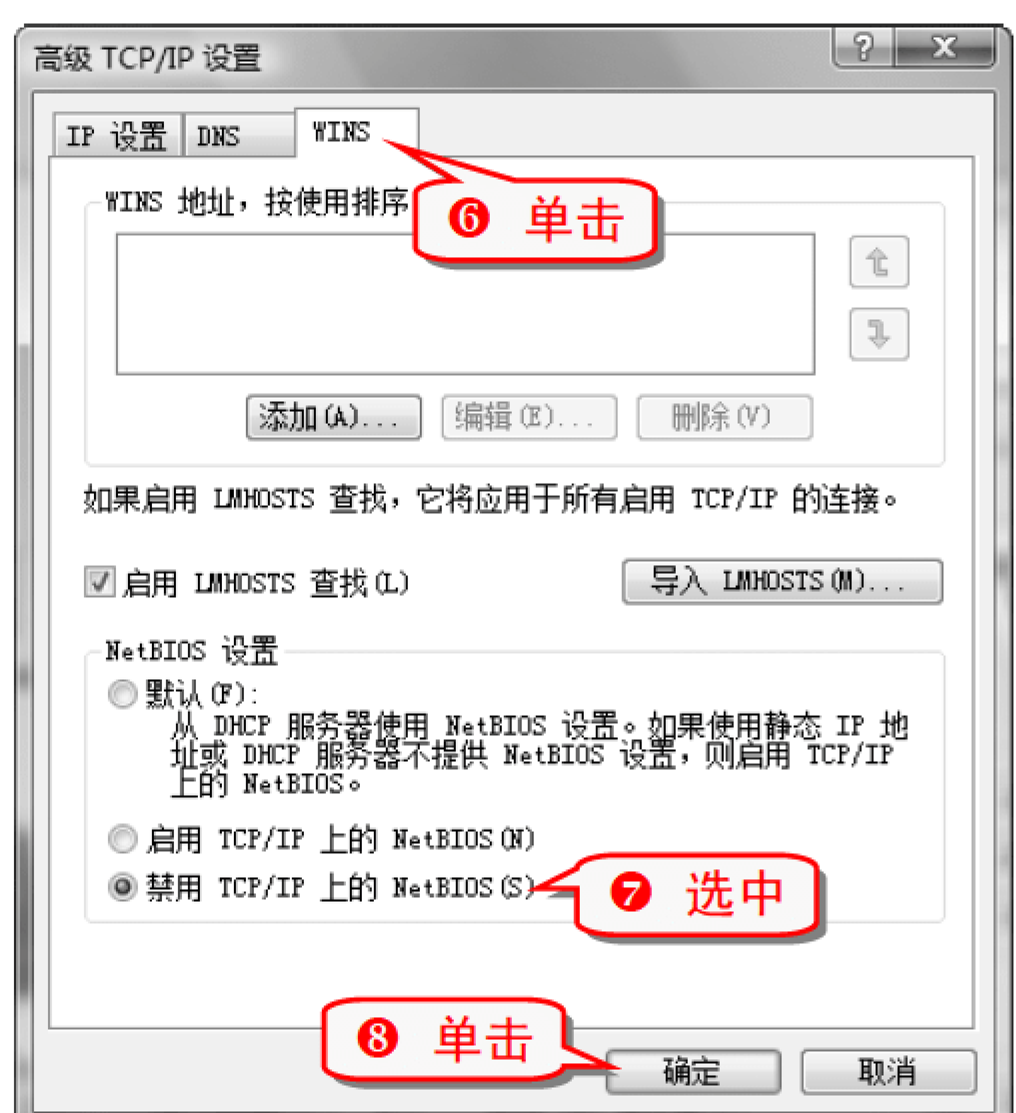












知　识　补　充




NBT 是一个网络协议，即 net bios over TCP/IP，用于文件和打印共享服务。

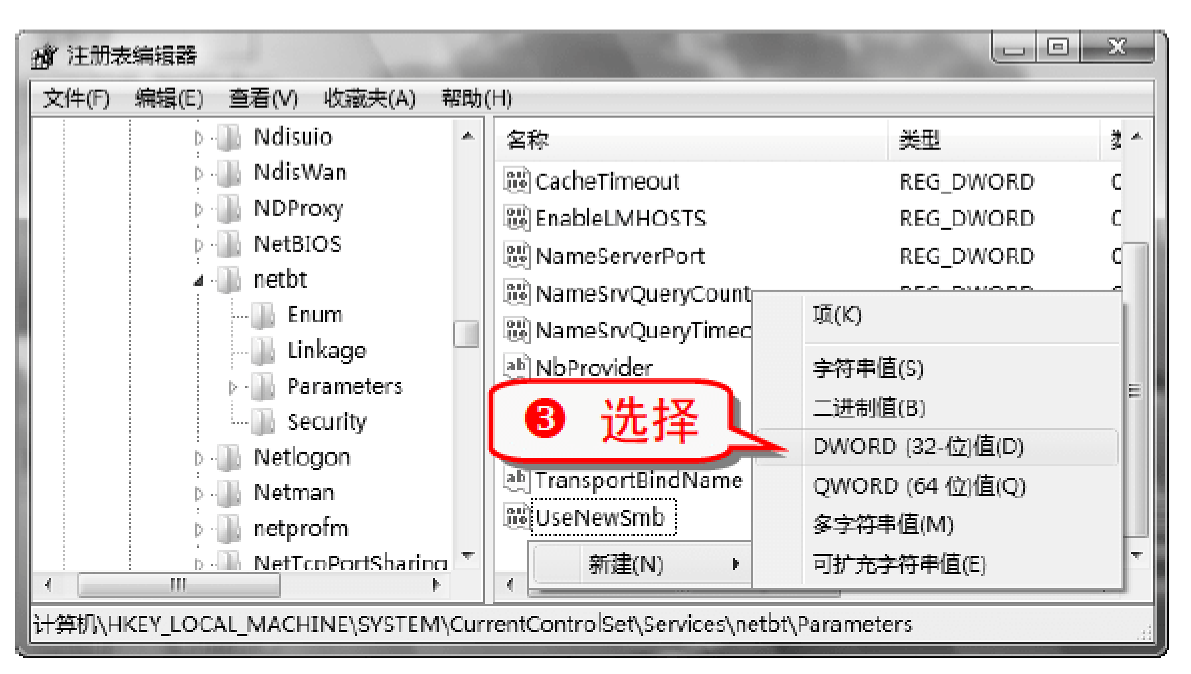
(4) 屏蔽 445 端口

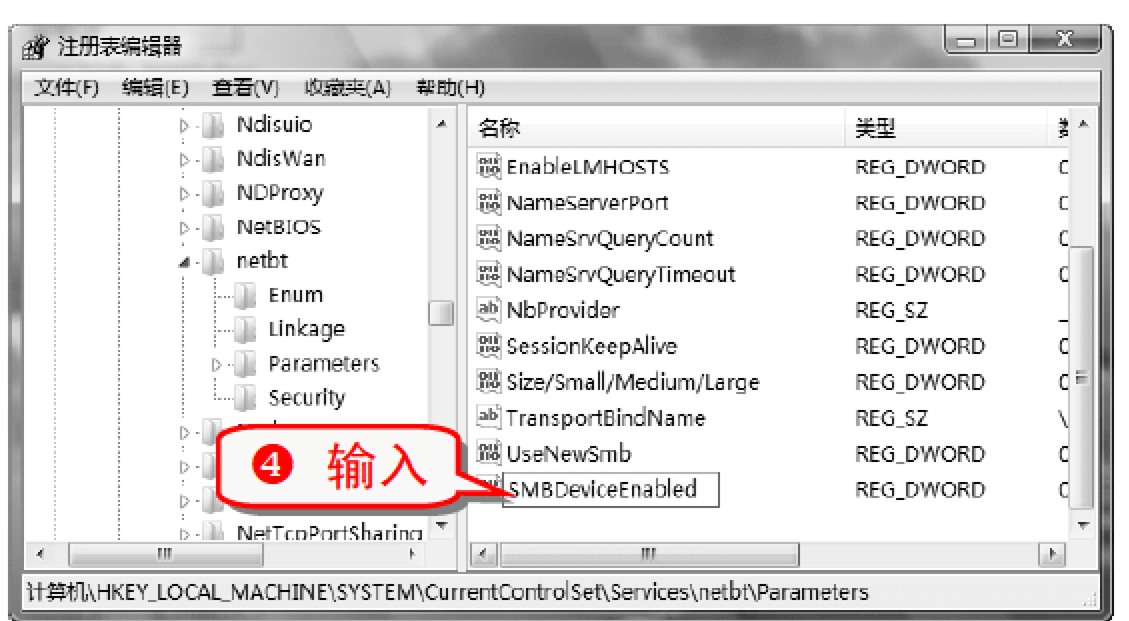
没有 445 端口的支持，是无法建立 IPC$连接的，因此屏蔽 445 端口同样可以阻止 IPC$入侵。

445 端口可以通过修改注册表来屏蔽。

❶ 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netbt\Parameters 分支。

❷ 右击右侧窗格空白处。







注　意　事　项



屏蔽掉以上两个端口，当前电脑也将无法与他人建立 IPC$连接。

举　一　反　三



除了在系统中屏蔽端口外，还可以通过下面的两种方法来防范 IPC$的入侵。

- 安装防火墙进行端口过滤。
- 设置复杂密码，防止通过 IPC$穷举出密码。

技巧213　巧用 MBSA 检测系统安全级别

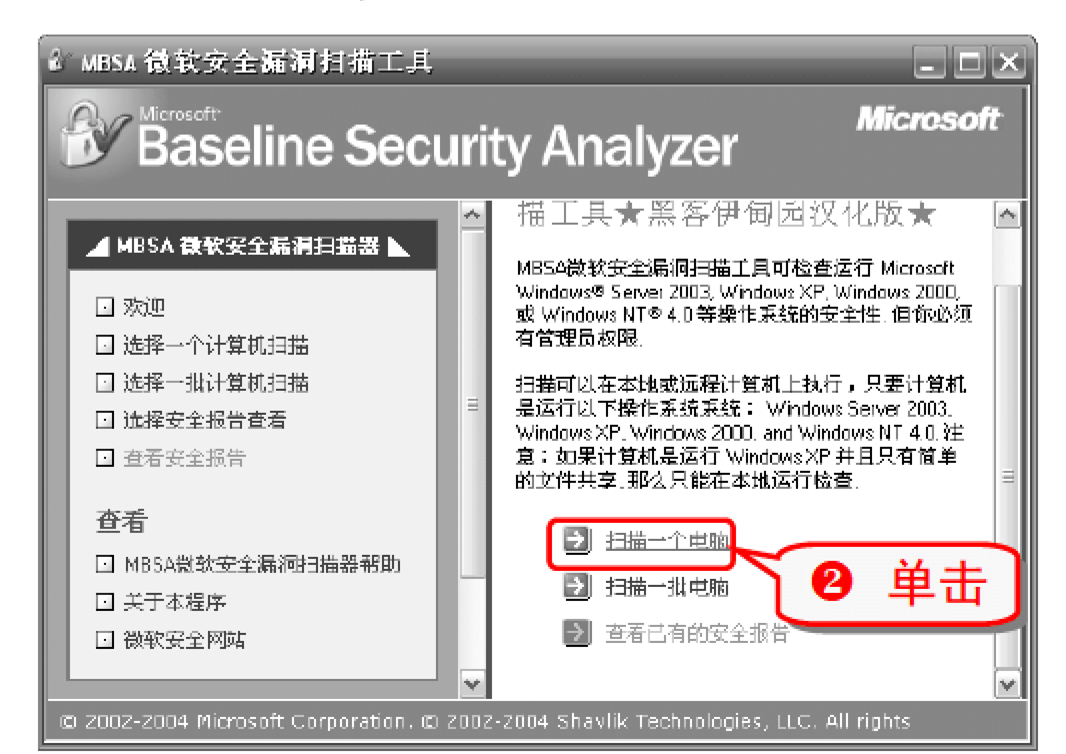
MBSA(Microsoft Baseline Security Analyzer)是一款 Windows 系统安全漏洞检测工具，可以对本机进行安全检测。

安装运行之后会出现如下图所示的主界面。



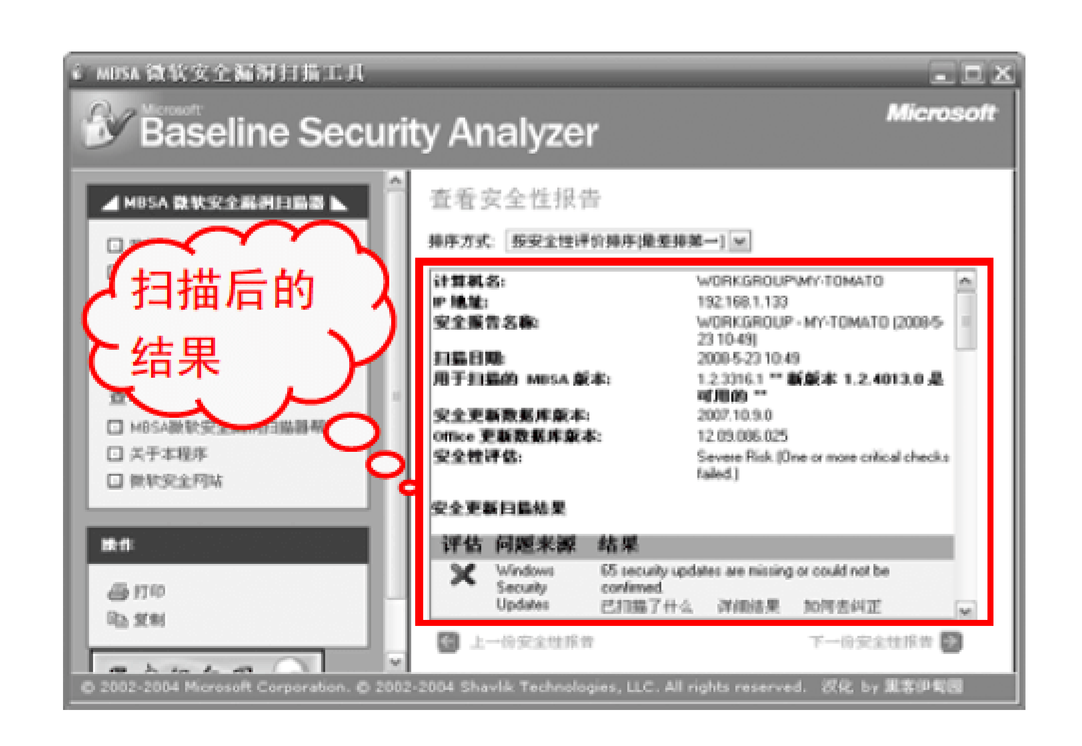
下面介绍对当前电脑进行安全检测的操作步骤。

❶ 运行 MBSA 主界面。









技巧214 巧用“跳板”

“跳板”是指达到入侵目标的一个中间工具，主要指的是代理服务器或者安全措施较差容易受到入侵攻击和控制的“肉鸡”。

黑客通过网络控制这些安全措施较差的电脑，然后实施入侵真正目标电脑的操作，在被入侵的目标电脑日志中，记录的是“跳板”在入侵的信息，而非真实的黑客电脑。

“跳板”可以有很多级，级数越多，追查黑客真实身份的难度也就越大。在实际的状况下，采用一定量的“跳板”后，由于网速过慢会造成操作无法顺利实现，所以“跳板”的级数是有限制的。

代理服务器的获得非常简单，互联网上有很多现成的代理服务器，在一些网站或者软件中，专门提供了这些代理服务器的地址。“肉鸡”则不是现成的，通常需要黑客自己进行查找、入侵，然后进行控制。

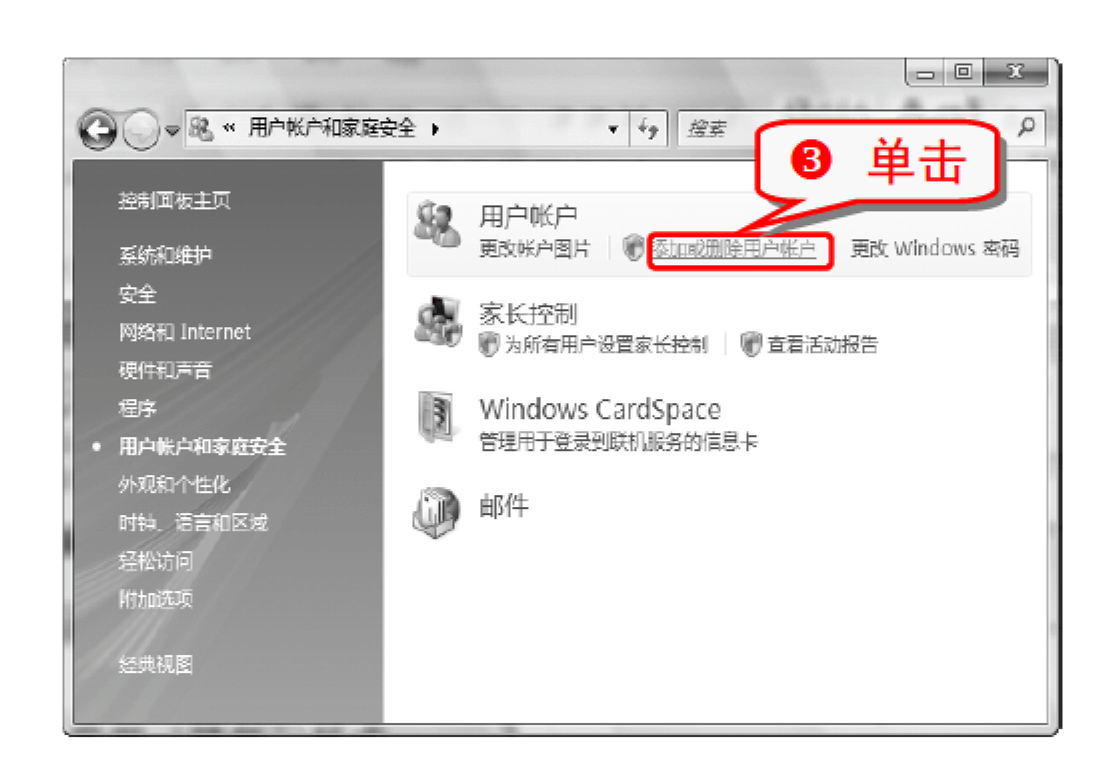
技巧215 降低 Administrator 用户权限

在 Windows 操作系统中，Administrator 是拥有最高权限的用户，通过正常的登录模式是无法看到的，而且 Administrator 用户的初始密码是空的，如果没用安装防火墙，黑客很容易通过 Administrator 账户入侵电脑。

❶ 选择“开始”→“控制面板”命令，打开“控制面板”窗口。













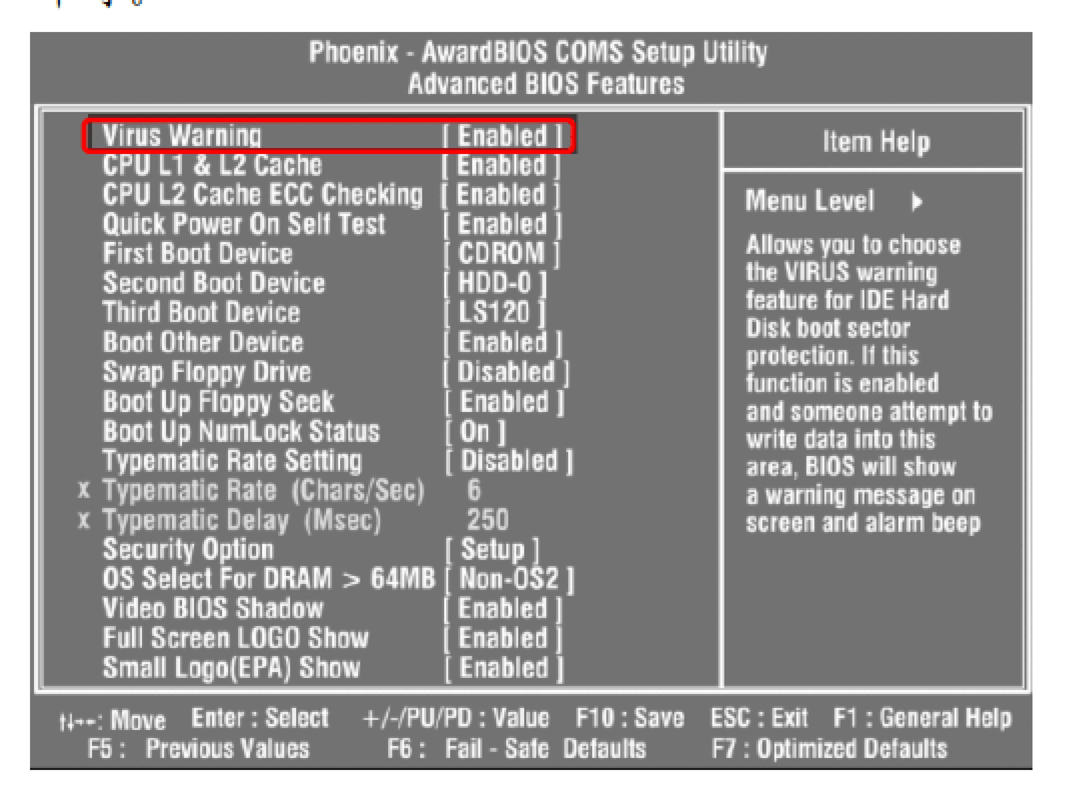
技巧216　巧用 BIOS 防病毒

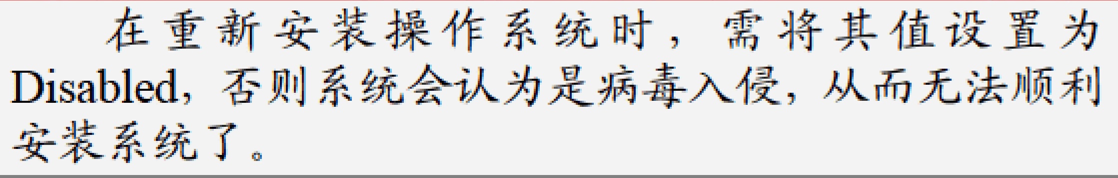
除了可以用杀毒软件进行病毒保护，也可以在 BIOS 中进行设置来防止病毒入侵。

❶ 启动电脑，然后按下 Del 键进入 BIOS 设置主界面。

❷ 选择 Advanced BIOS Features(高级 BIOS 功能设置)功能项，按下 Enter 键。

❸ 将 Virus Warning(病毒保护)功能项设置为 Enabled 即可。





在重新安装操作系统时，需将其值设置为 Disabled，否则系统会认为是病毒入侵，从而无法顺利安装系统了。

技巧217　杜绝 JPEG 图片病毒的侵害

JPEG 图片漏洞存在于微软提供的一个用于图形开发的动态链接库(Gdiplus.dll)中，电子图片文件会被该系统文件使用，从而被加入各种病毒代码。

(1) 使用专杀工具

❶ 到 http://db.kingsoft.com/download/othertools/DubaTool_JPEG.exe 去下载一个“JEPG 病毒及漏洞检测”专杀工具。

❷ 运行“JEPG 病毒及漏洞检测”病毒专杀工具。





金山毒霸“JEPG 病毒及漏洞检测”病毒专杀工具可以全盘扫描磁盘上的所有 Gdiplus.dll 文件，包括系统及第三方应用软件中的该文件。将存在漏洞的 Gdiplus.dll 文件找出来，并可自动将其修补。

(2) 到微软官方网站下载漏洞补丁

❶ 到微软官方网站下载没有漏洞的 Gdiplus.dll 文件。

❷ 选择“开始”→“所有程序”→“搜索”命令，启用高级搜索，在名称文本框中填写 Gdiplus.dll 进行搜索。

❸ 将从微软网站下载的 Gdiplus.dll 文件替换这些文件。

技巧218 利用 DiskState 全面监控磁盘空间

DiskState 可以检查出磁盘上有多少重复文件，记录每一次安装、卸载和删除等操作在系统文件夹里发生的变化。DiskState 还可以清晰地列出磁盘上各文件夹占用空间的大小比例。

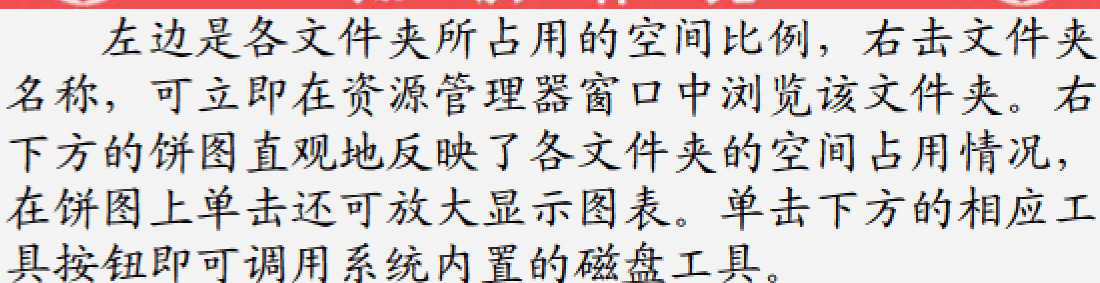
(1) 全面了解磁盘信息

运行 DiskState 以后，在其主界面上会以简洁明了的方式显示各硬盘分区以及可移动磁盘和网络映射磁盘的各种信息。



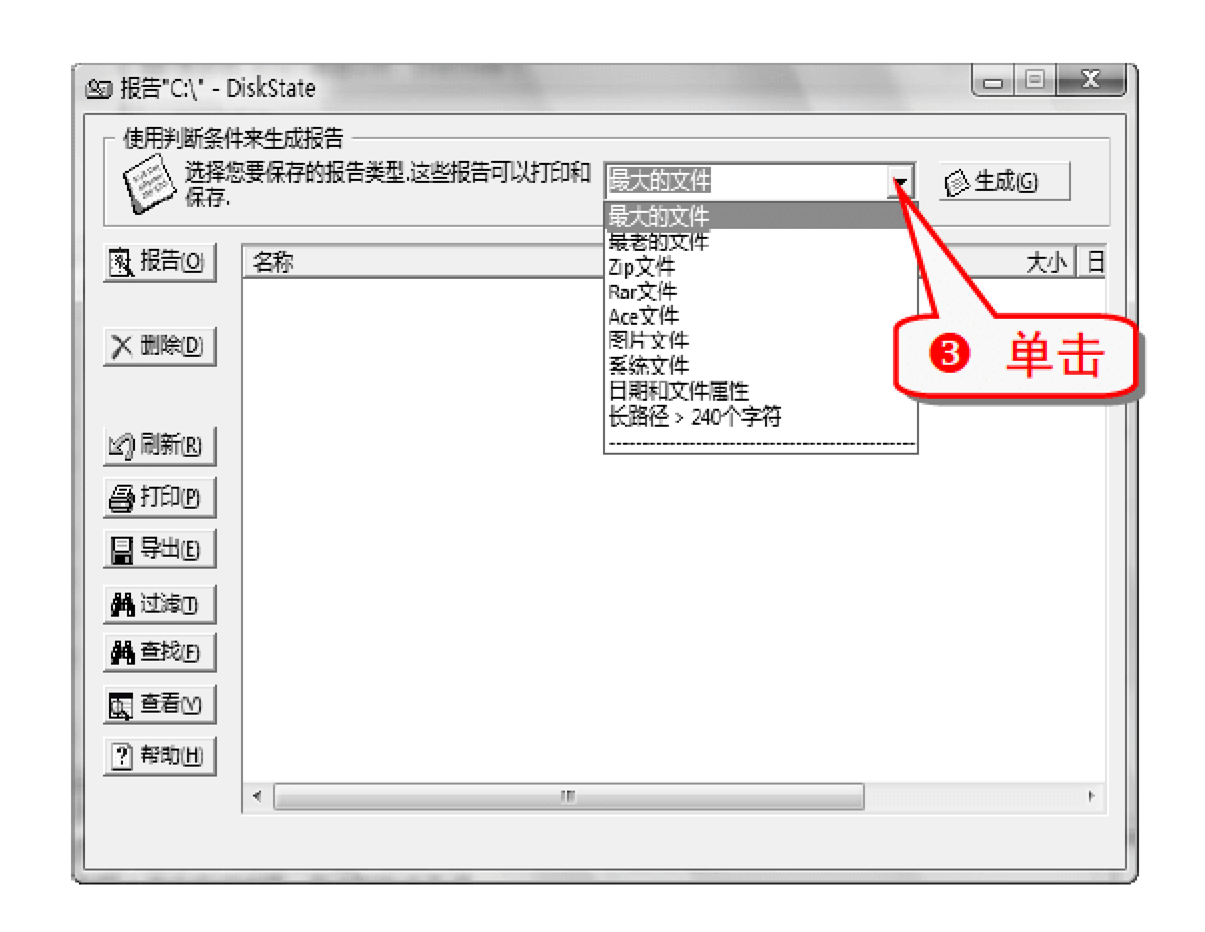
随后出现下图所示的窗口。





左边是各文件夹所占用的空间比例，右击文件夹名称，可立即在资源管理器窗口中浏览该文件夹。右下方的饼图直观地反映了各文件夹的空间占用情况，在饼图上单击还可放大显示图表。单击下方的相应工具按钮即可调用系统内置的磁盘工具。

❷ 单击“报告”按钮，会弹出报告文件磁盘状态的窗口。



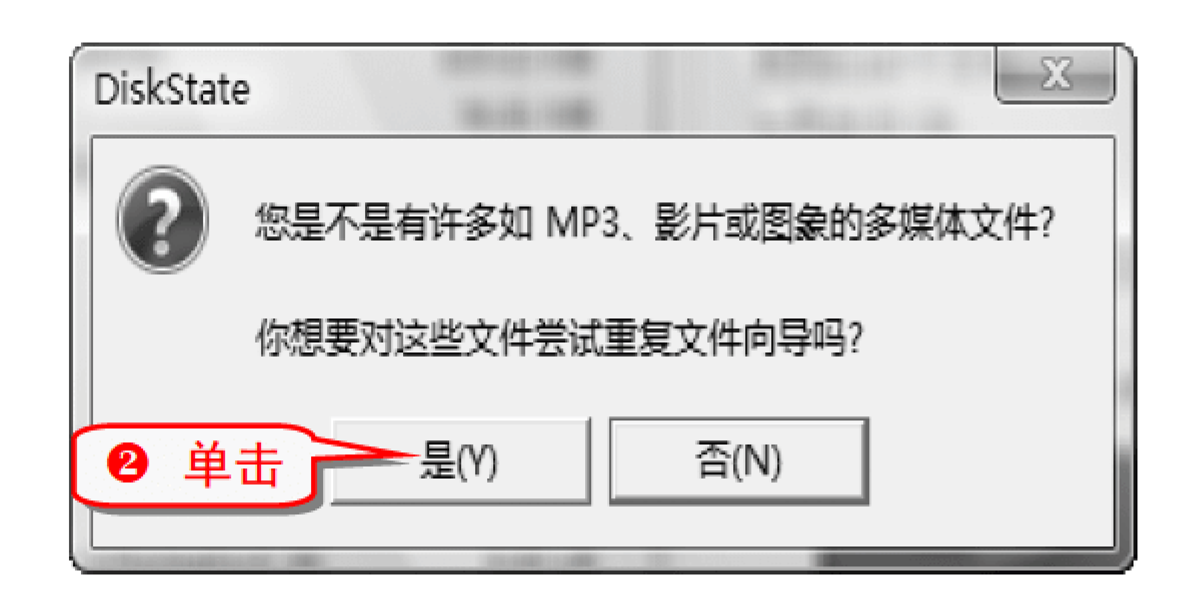
专 家 坐 堂

从该窗口中可以迅速找到磁盘上体积最大或者建立时间最早的文件，想知道这个分区上究竟有多少个系统文件、多少个图片文件、多少个 ZIP 或 RAR 压缩文件等，都可以利用“报告”列出来。在“使用判断条件来生成报告”下拉列表中选择报告的类型，单击“生成”按钮，就会显示出符合报告条件的文件列表，还可以方便地打印出来。

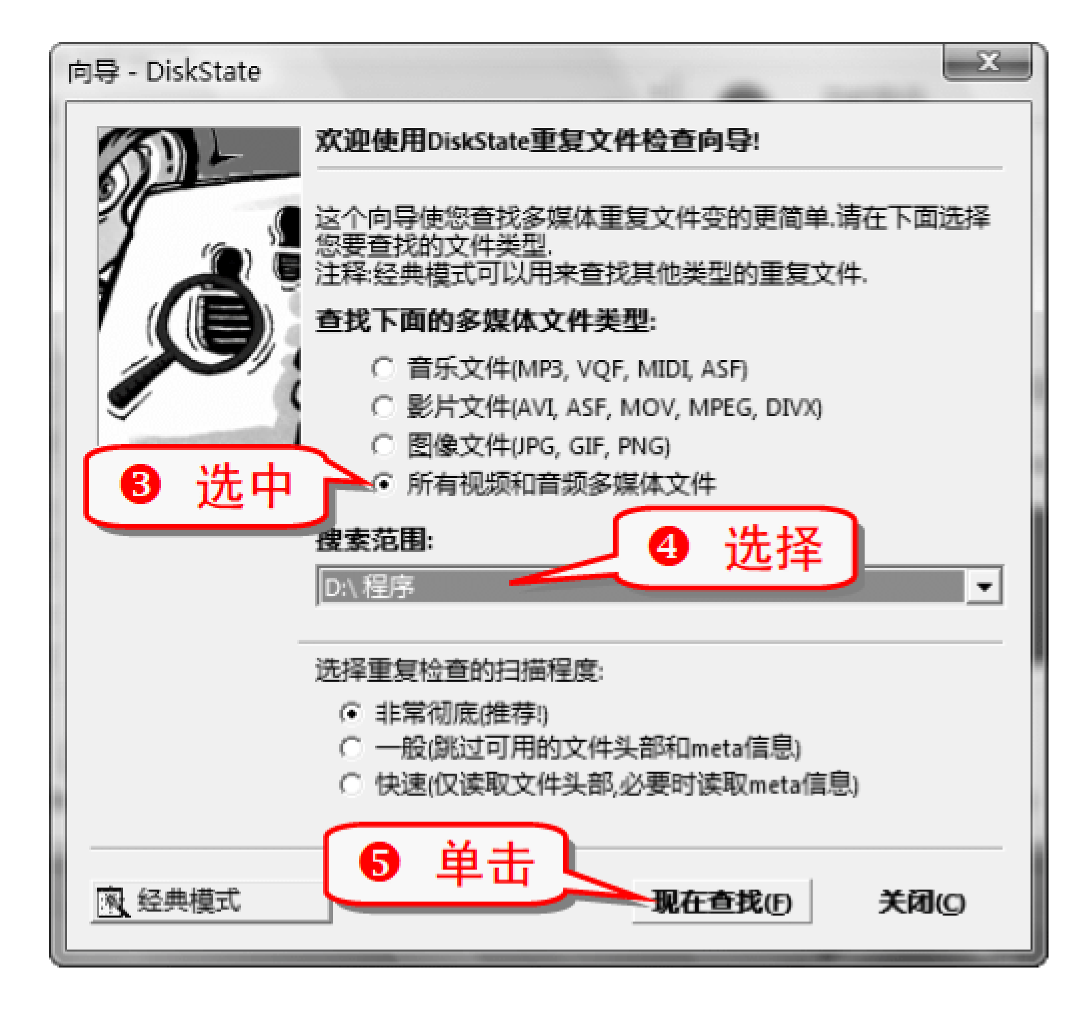
(2) 让重复文件无处藏身

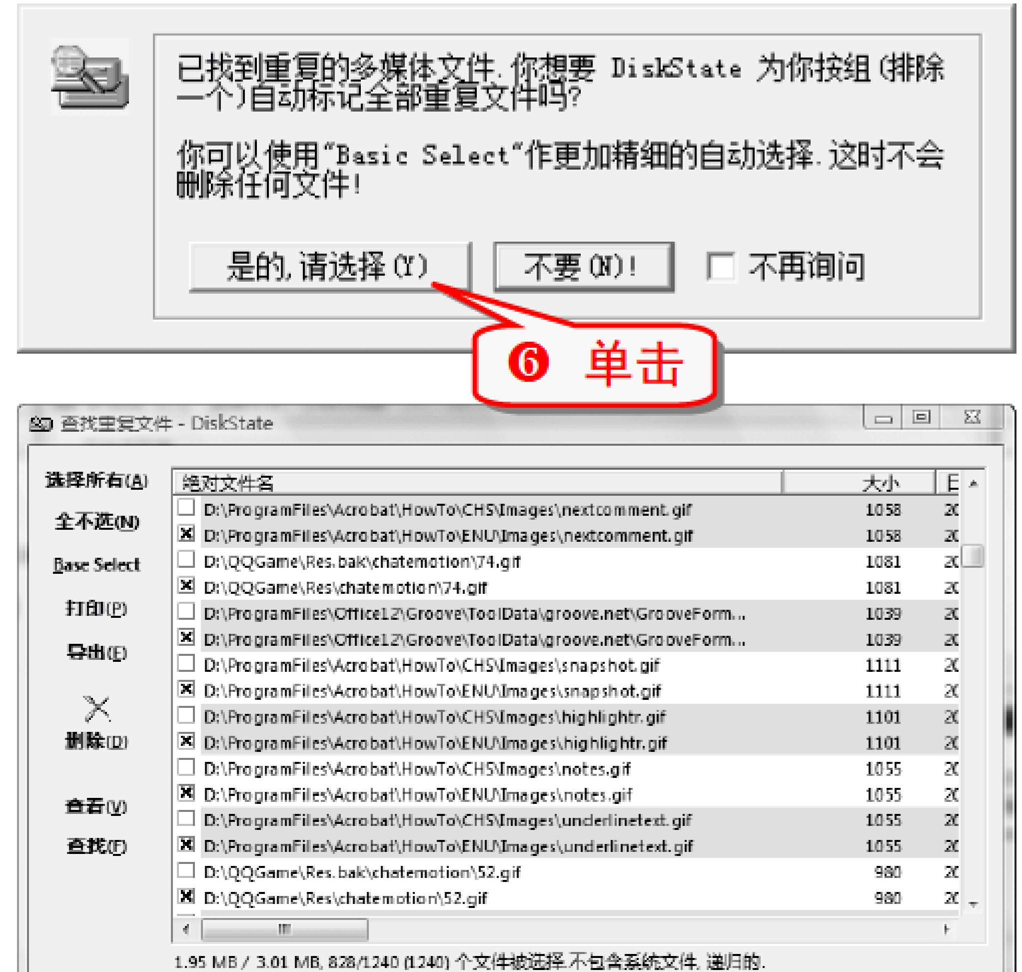
由于一些文件随意存放，用户在很难找到的情况下会重新做一份文件。导致有大量的重复文件。影片、音乐和图片这类文件最容易出现重复，DiskState 的“重复文件查找”功能专门针对这三类文件。

❶ 在软件主界面上单击“重复文件”按钮。







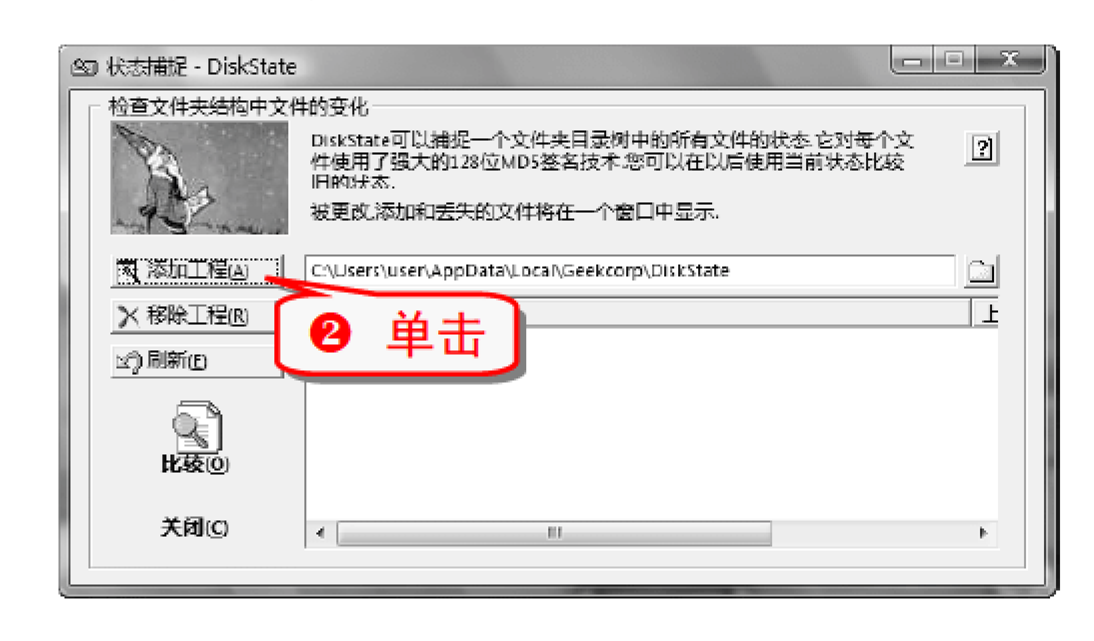


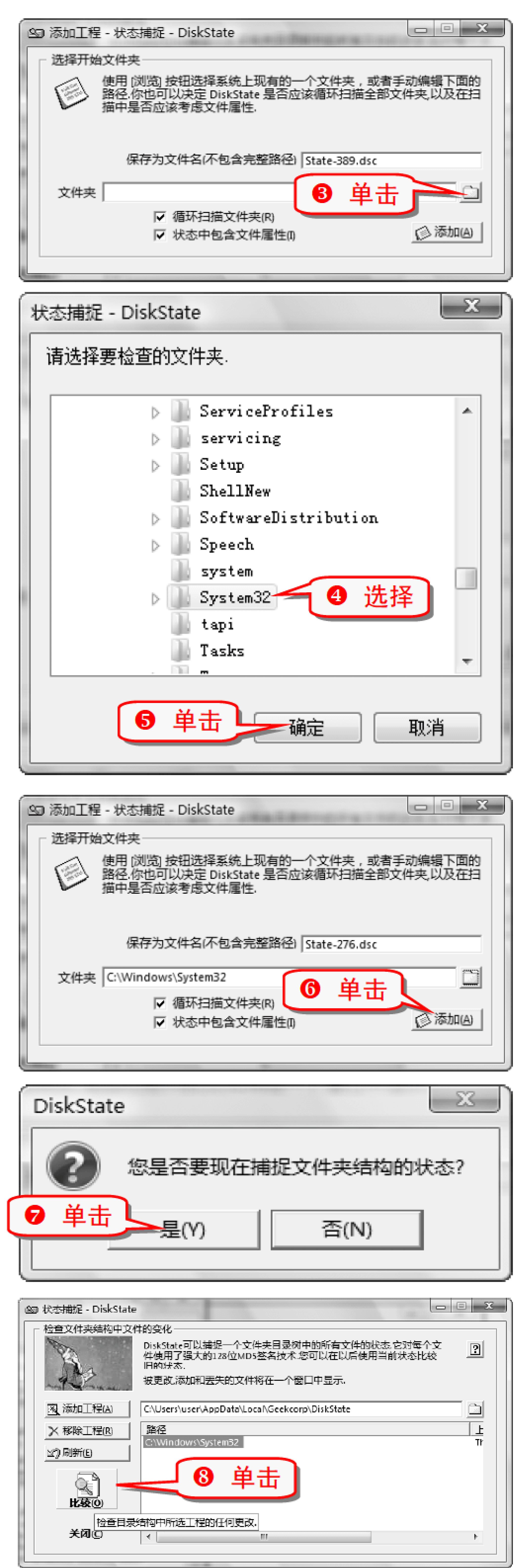
❼ 在结果对话框中有选择地删除重复的文件。

(3) 监控文件夹的改变

软件安装或卸载后 Windows 系统目录中会被写入一些文件，这些操作都是在后台运行的，用户无法知道系统目录中发生什么变化。利用 DiskState 只需在系统改变前保存当前状态，即可在软件安装或卸载后进行比较，并给出详细的比较结果。

❶ 在主界面上单击“比较”按钮。





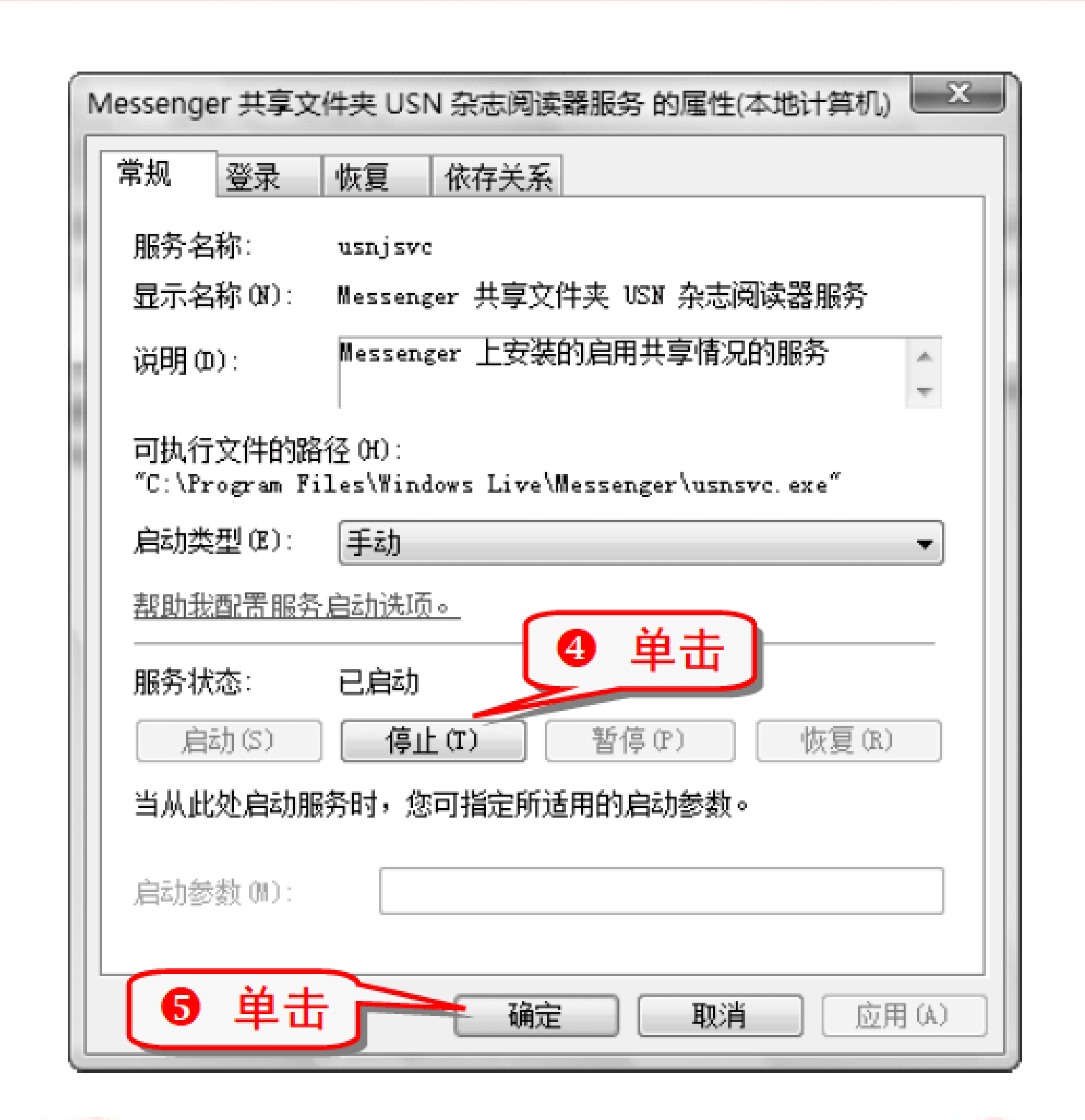
❾ 最后给出详细的比较结果，执行相应操作。

技巧219 在 Windows Vista 下停止信使服务

Windows Vista 系统提供的信使服务常常被黑客利用，在一些局域网扫描工具中，都提供了利用信使服务发送信息的功能，如果将信使服务启用，很容易受到恶意的骚扰。进行下列设置可以防止骚扰。

❶ 右击“计算机”图标，在弹出的“快捷菜单”中选择“管理”命令。





知 识 补 充

信使服务，传输客户端和服务器之间的 Net Send(发送消息)和 Alerter(报警器)服务消息。此服务与 Windows Messenger 无关。默认情况下，“信使服务”是打开的，所以一旦计算机连接到 Internet，一些网站(包括厂商网站)就可以通过该服务发送一些信息，并在用户电脑上弹出一个名为“信使服务”的对话框。



专题八　玩转远程控制与黑客扫描

内容导航

远程控制功能能让朋友远在千里之外帮助自己解决电脑上遇到的问题，但是远程控制同样也是黑客攻击常用的途径。掌握远程控制软件和扫描工具的用法可以有效地防范黑客的攻击。

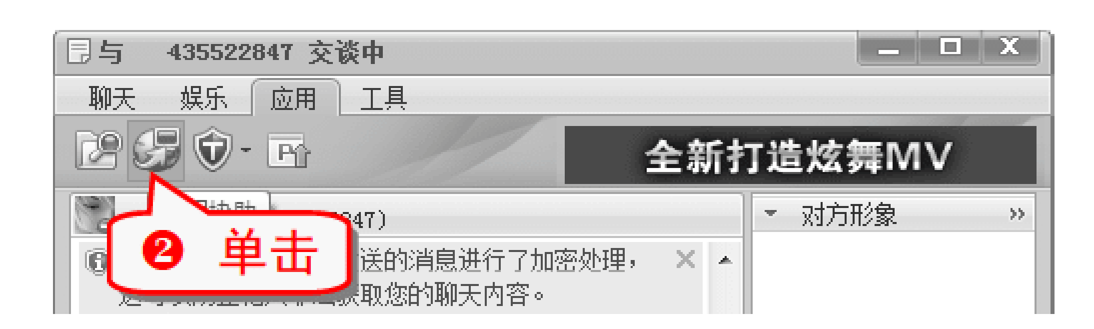


- 远程协助使用技巧
- 远程桌面连接技巧
- 网络人使用全攻略
- Radmin 使用全攻略
- 流光使用全攻略
- S 扫描器使用技巧

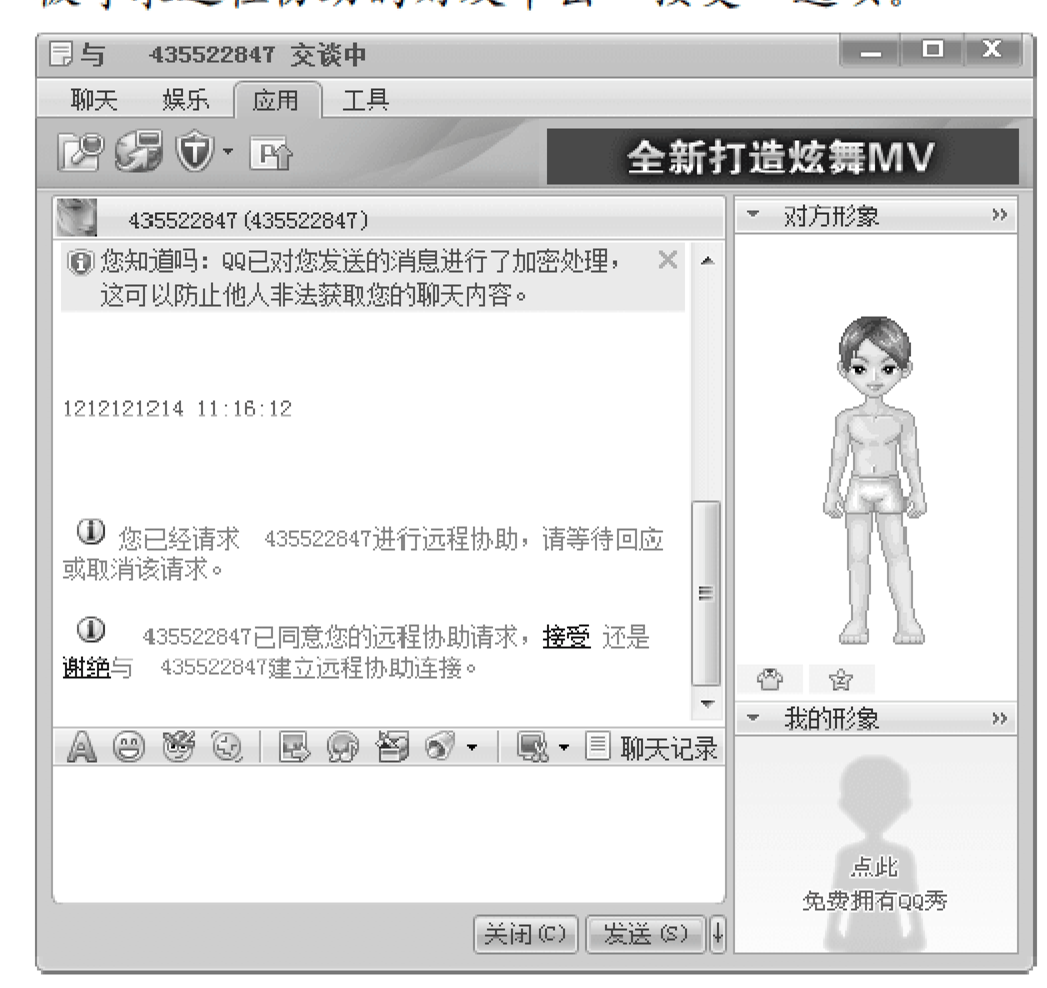
技巧220　利用 QQ 实现远程控制

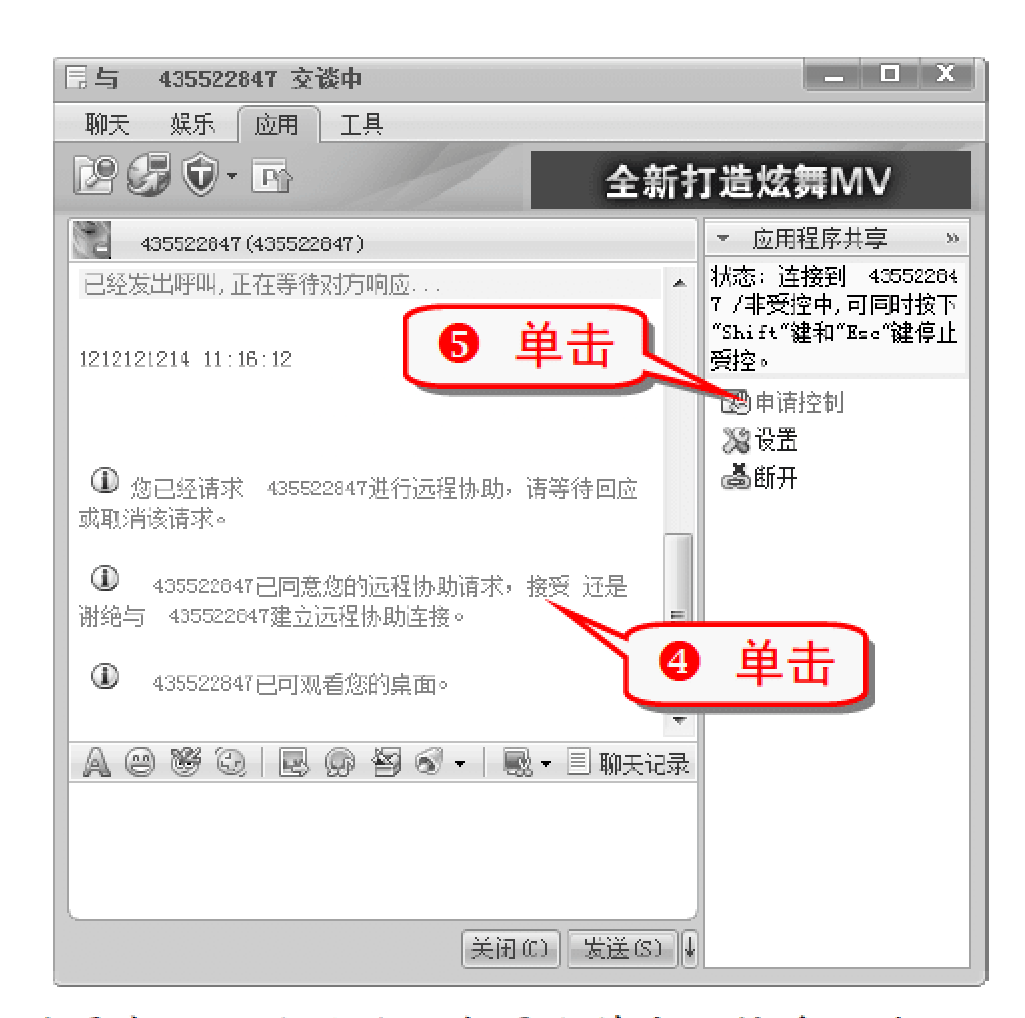
电脑出现问题，可以通过QQ远程协助寻求别人的帮助。

❶ 打开想要寻求远程协助的 QQ 好友对话框。



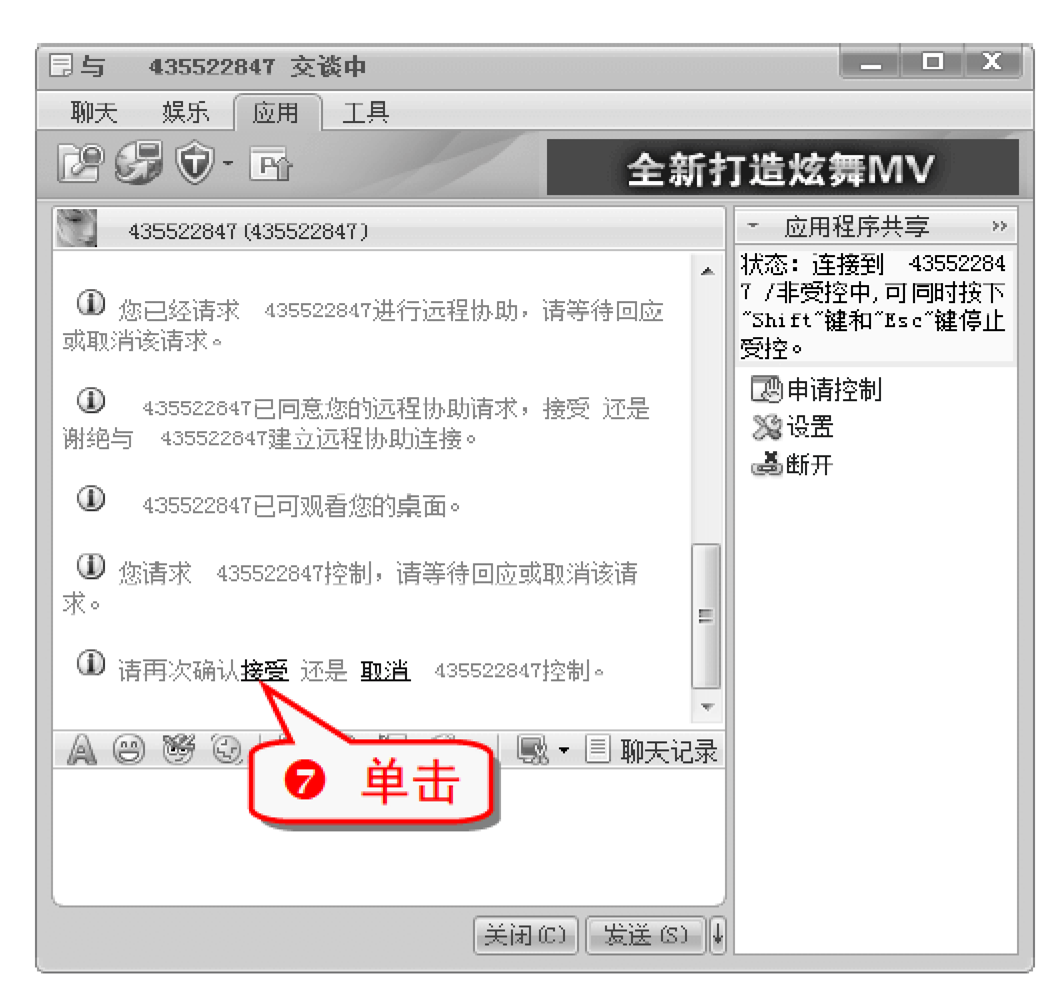
❸ 被寻求远程协助的好友单击“接受”选项。





❻ 被寻求远程协助的好友再次单击“接受”选项。





技巧221 在 Windows Vista 系统下实现远程协助

Windows Vista 系统自带远程协助功能，可以利用这个功能向好友发送远程协助请求。

(1) 发送远程协助请求

❶ 选择“开始”→“所有程序”→“维护”→“Windows 远程协助”命令。



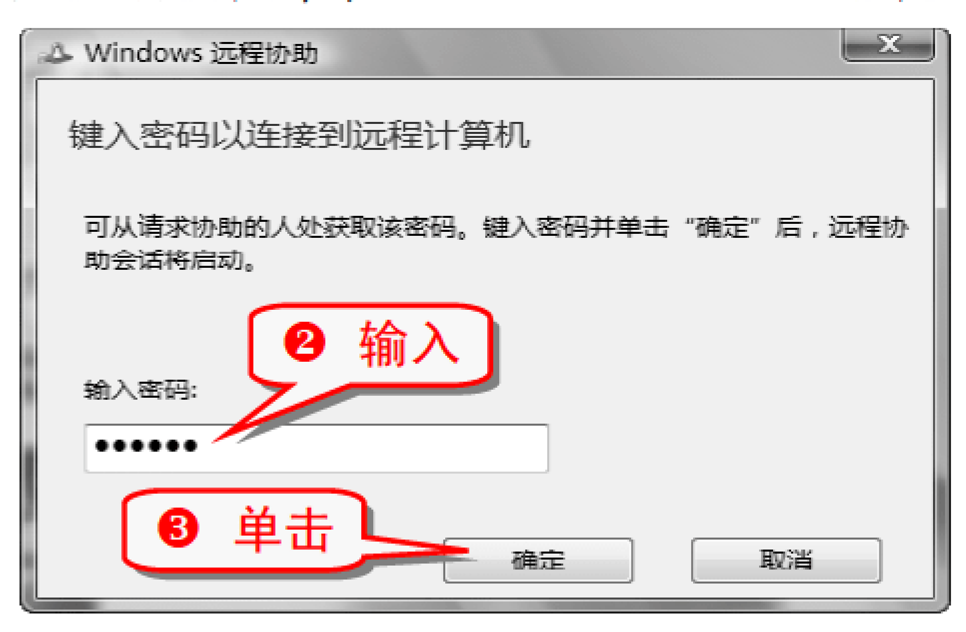




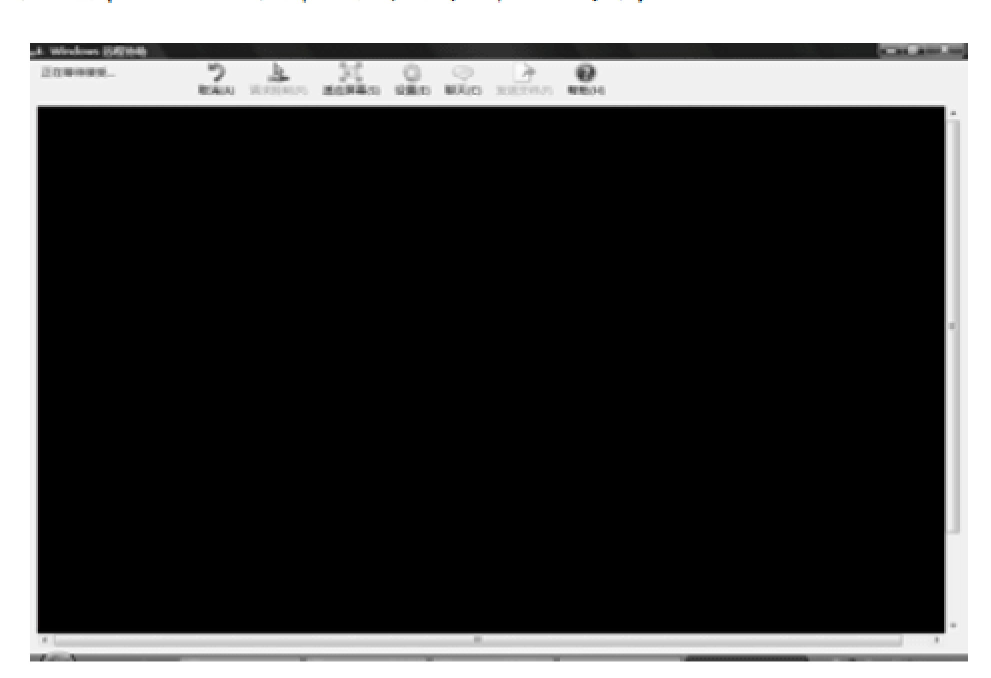
❺ 在桌面上生成 Invitation.msrcincident 文件之后，通过 QQ 或 E-mail，将密码传给好友。

(2) 响应远程协助请求

❶ 好友双击接收到的 Invitation.msrcincident 文件。



❹ 好友桌面上会弹出下图所示的窗口。



❺ 此时当前桌面上会弹出如下对话框。



❼ 好友发出“请求控制”邀请。





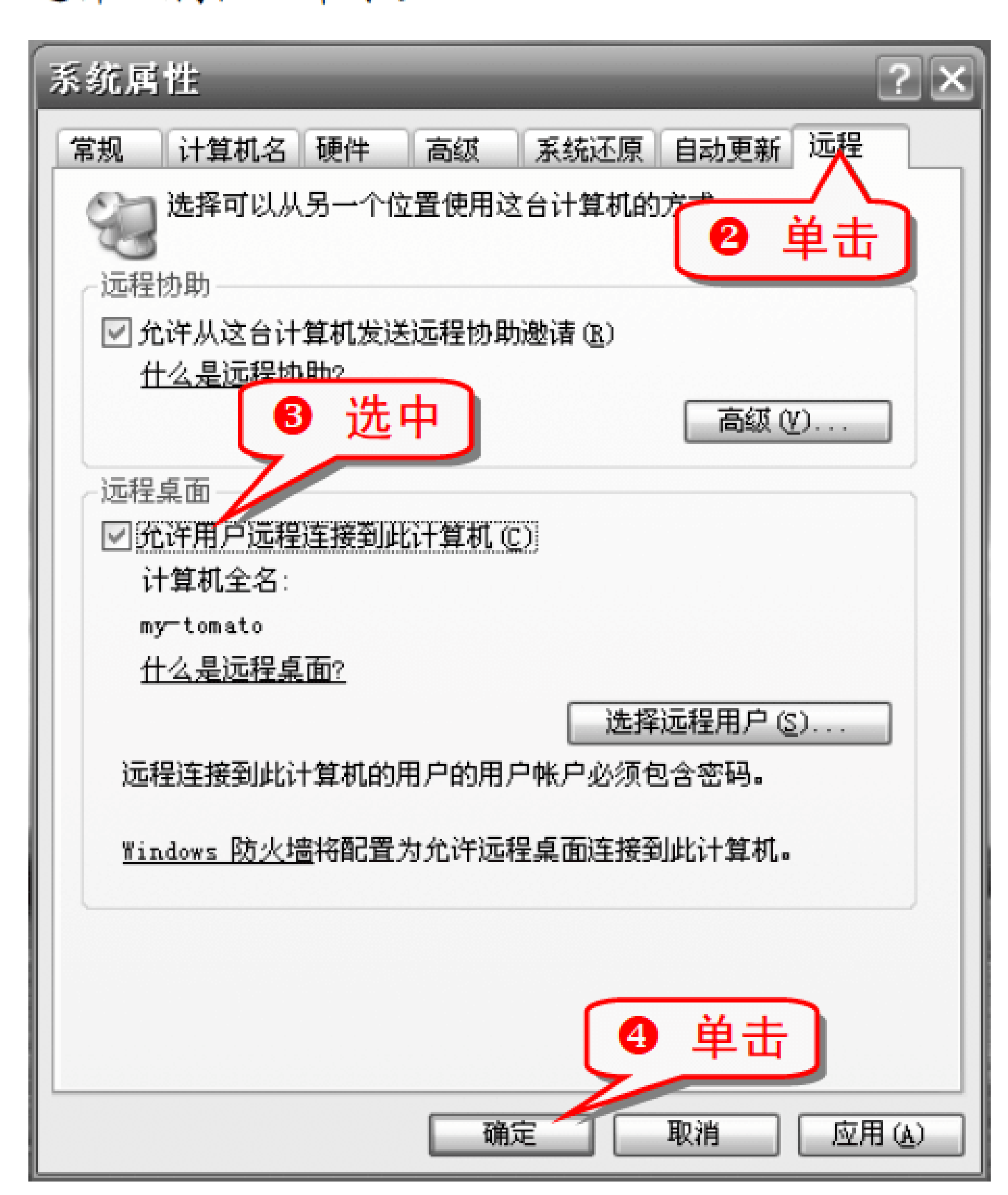
❾ 当前电脑允许对方控制要求。



技巧222　Windows Vista 连接 Windows XP 远程桌面

如果家里有两台电脑，一台是 Windows XP 的系统，一台是 Windows Vista 的系统，可以在 Windows Vista 的系统中连接 Windows XP 的远程桌面。

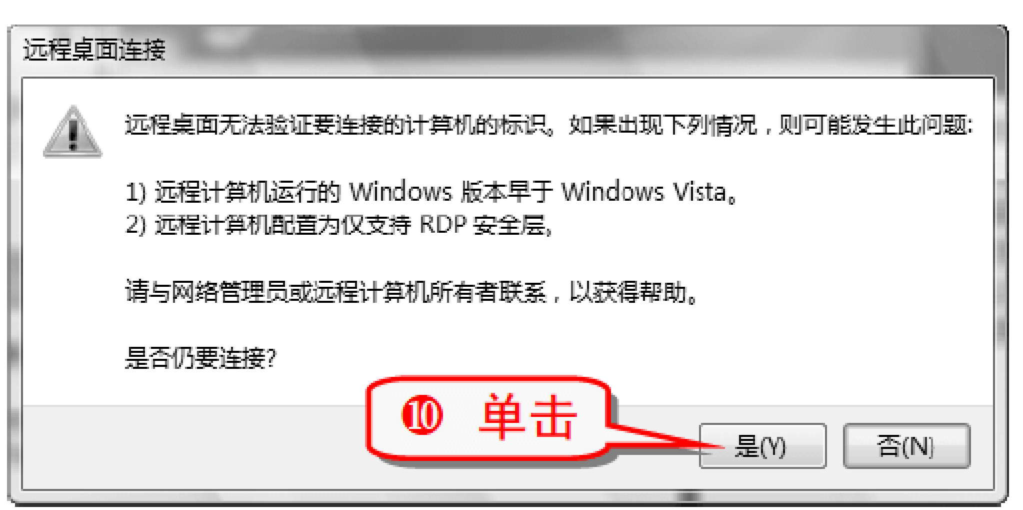
❶ 在 Windows XP 的系统中，右击“我的电脑”图标，选择“属性”命令。



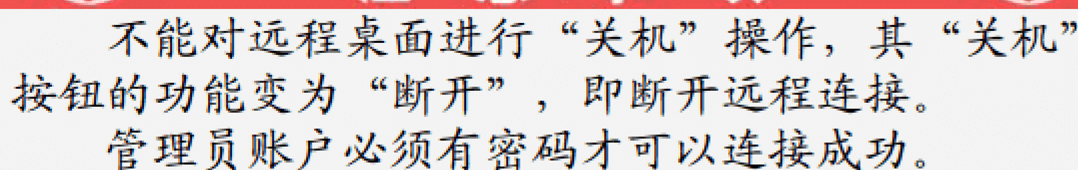
❺ 在 Windows Vista 系统中，选择“开始”→“所有程序”→“附件”→“远程桌面连接”命令。











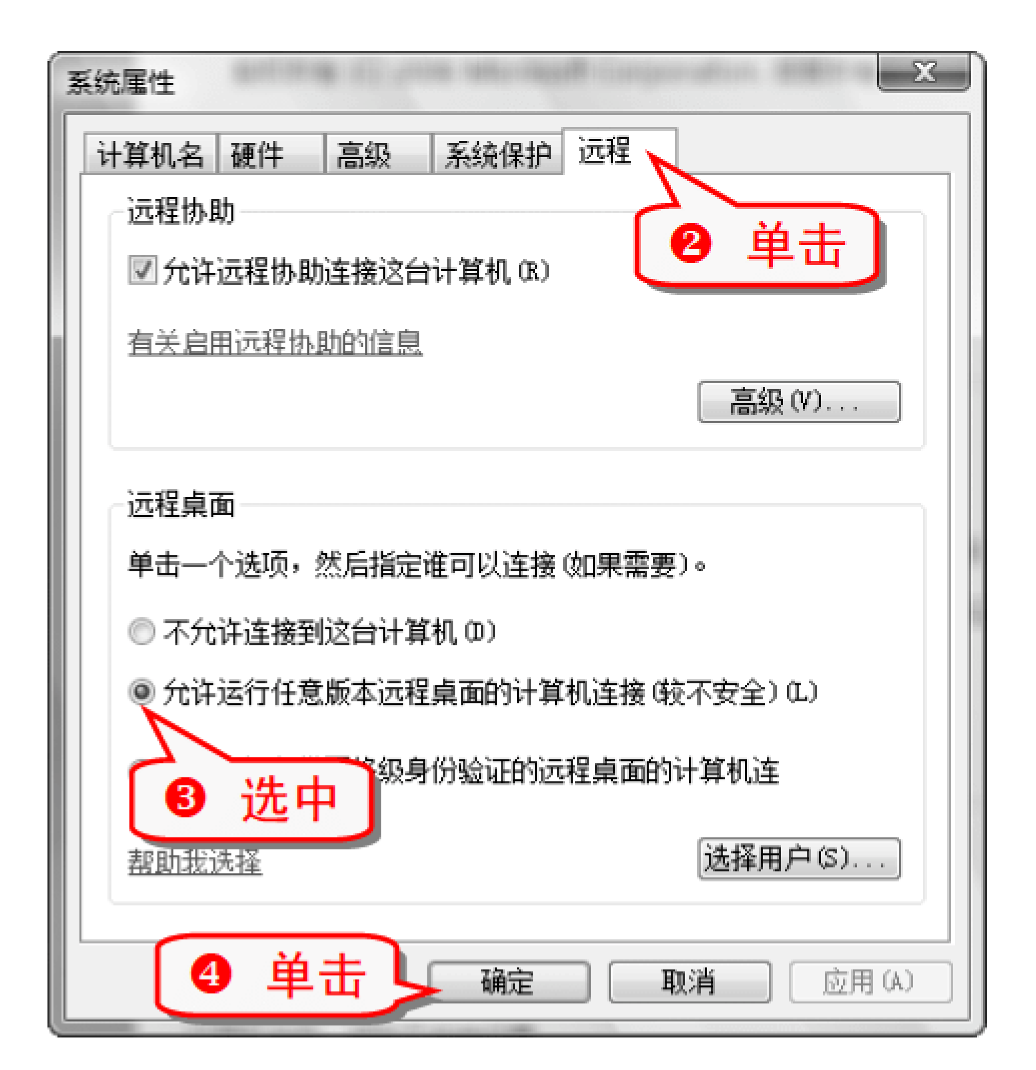
不能对远程桌面进行“关机”操作，其“关机”按钮的功能变为“断开”，即断开远程连接。

管理员账户必须有密码才可以连接成功。

技巧223　Windows XP 系统连接 Windows Vista 系统远程桌面

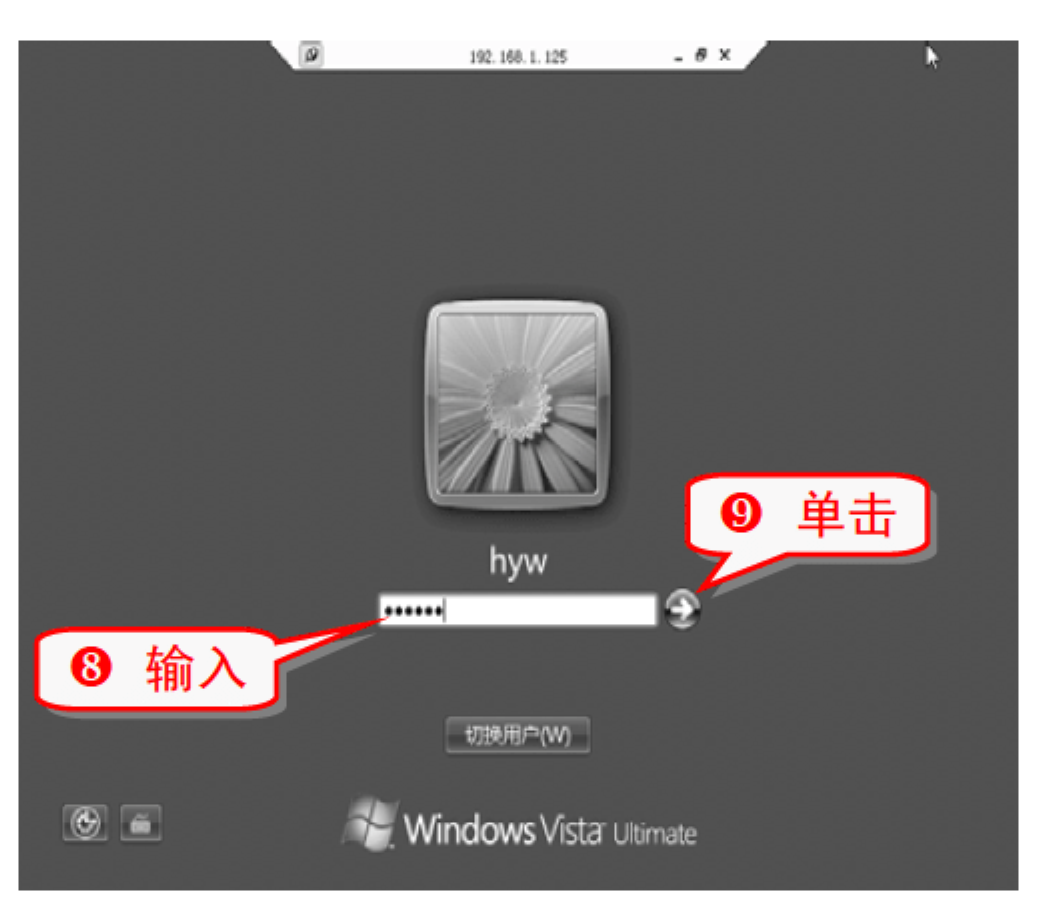
在 Windows XP 系统中连接 Windows Vista 系统的远程系统桌面的方法和在 Windows Vista 系统中连接 Windows XP 系统远程桌面的方法类似。

❶ 在 Windows Vista 系统中，右击“计算机”图标，选择“属性”命令，弹出“系统属性”对话框。











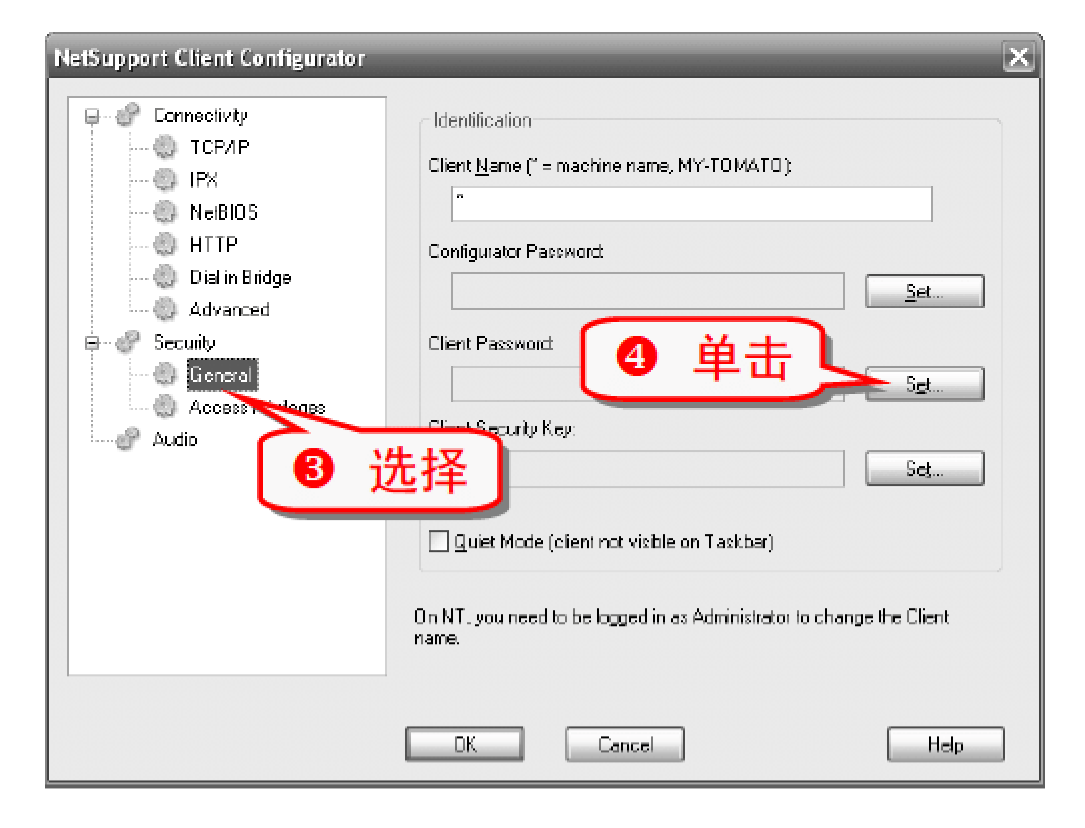
技巧224 巧用 NetSupport Manager

NetSupport Manager 将高级桌面管理功能与强大的 PC 远程控制结合在一起，支持 Windows XP 和 Windows Vista 系统，运行速度非常快。

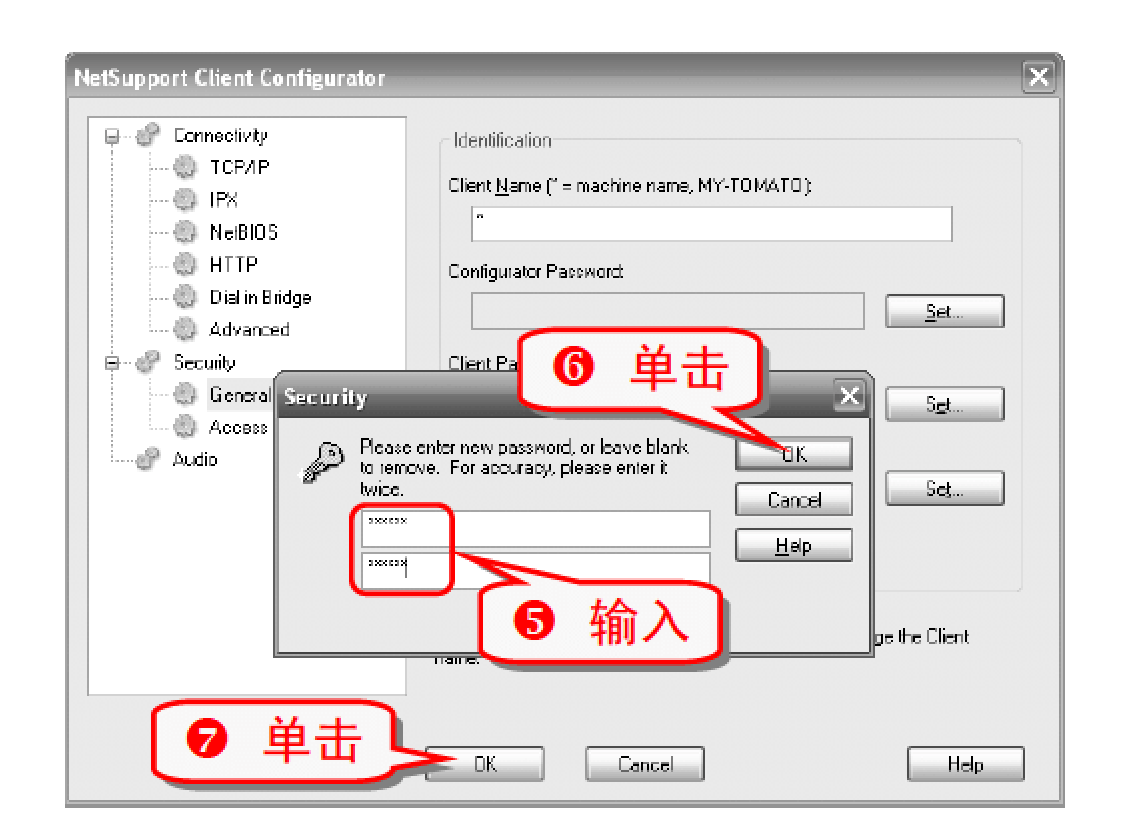
(1) 对 Windows XP 系统进行配置

❶ 在 Windows XP 系统中选择“开始”→“所有程序”→ NetSupport Manager → NetSupport Manager Configurator 命令。









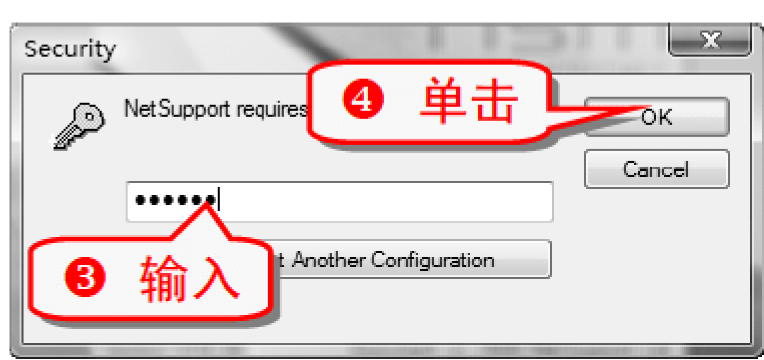
注　意　事　项

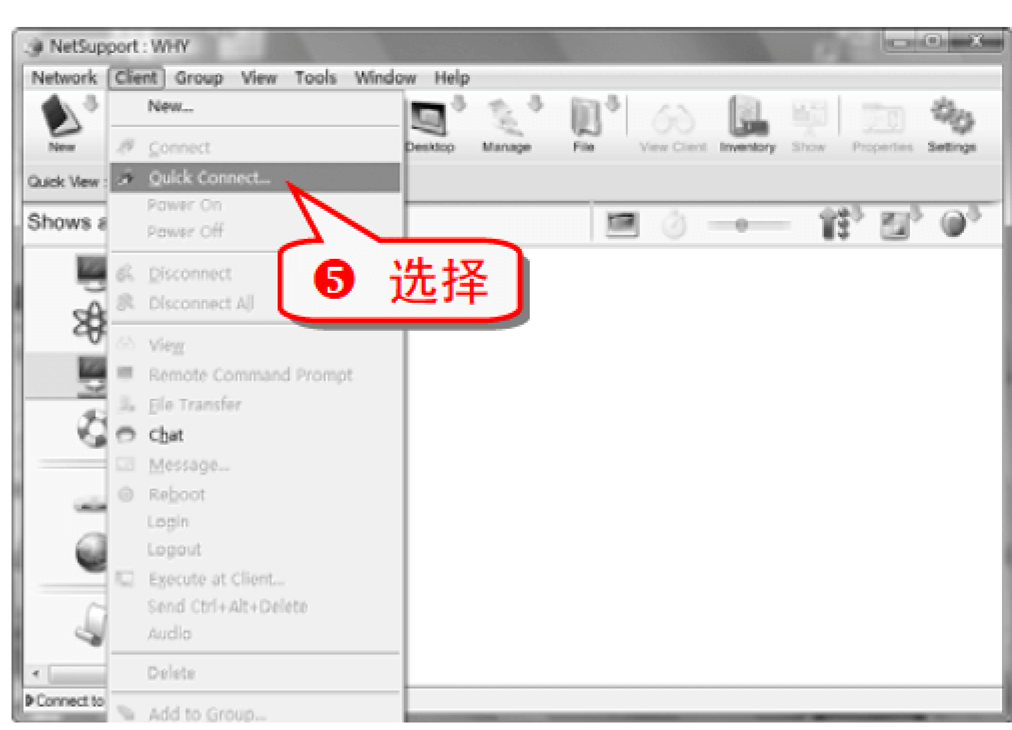
在 Windows Vista 系统中对 NetSupport Manager 进行配置的步骤和在 Windows XP 系统中的一样。

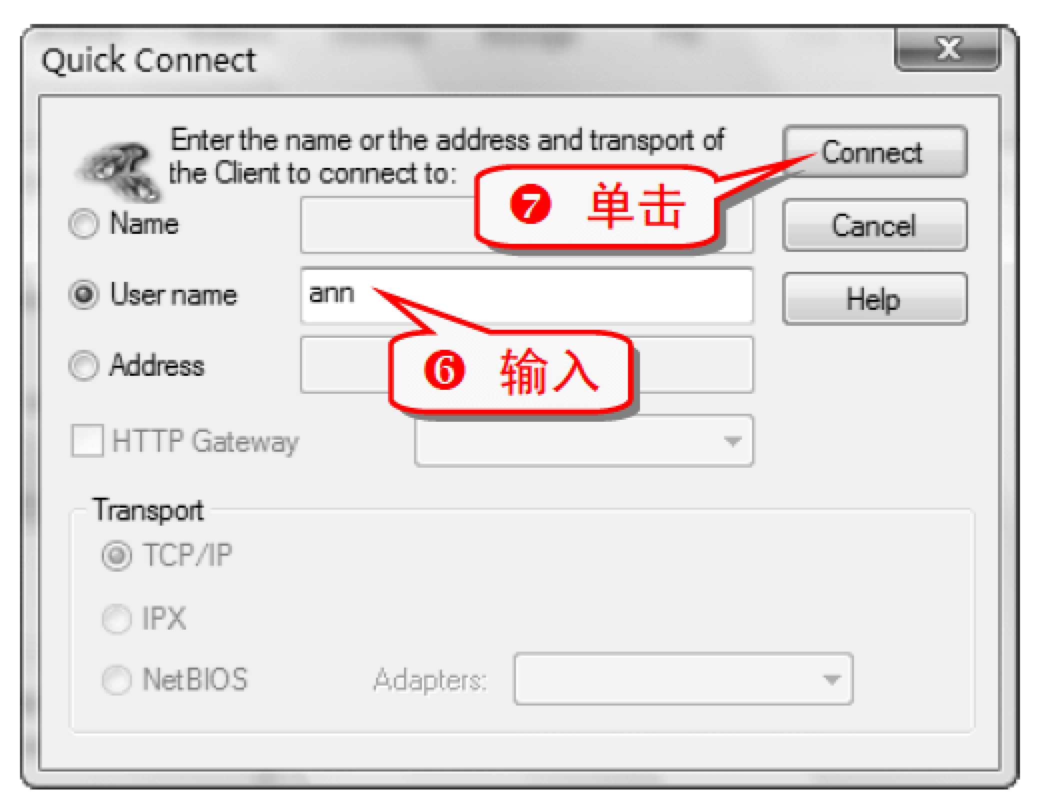
(2) 在 Windows Vista 系统中控制 Windows XP 远程桌面

❶ 选择"开始"→"所有程序"命令。

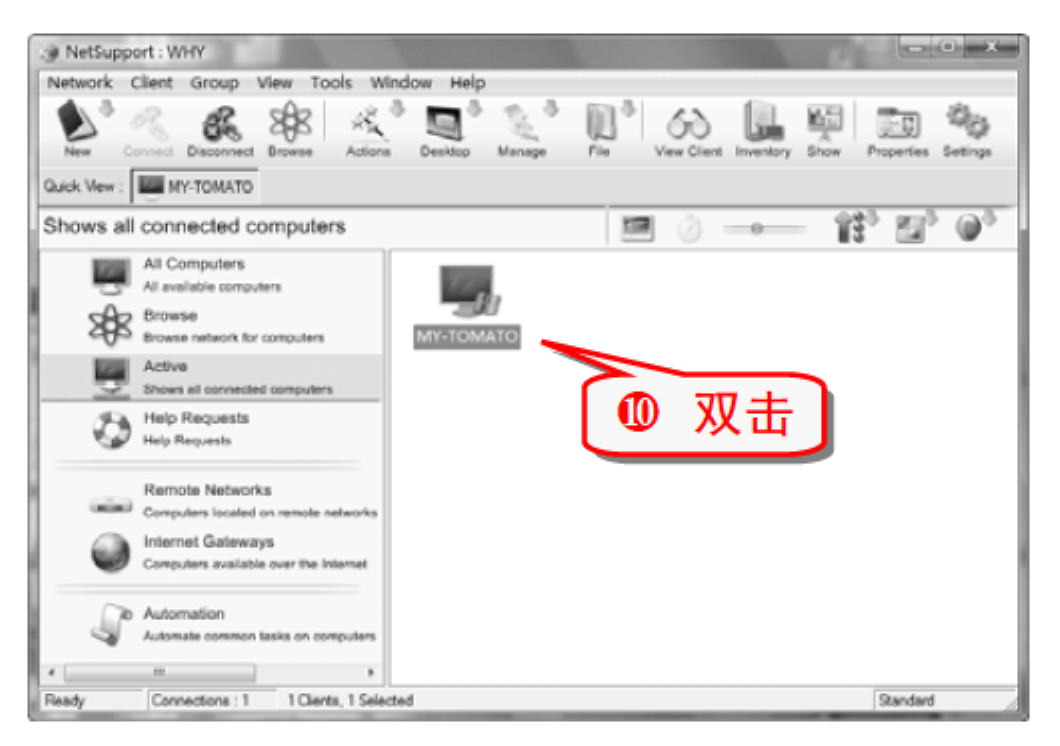


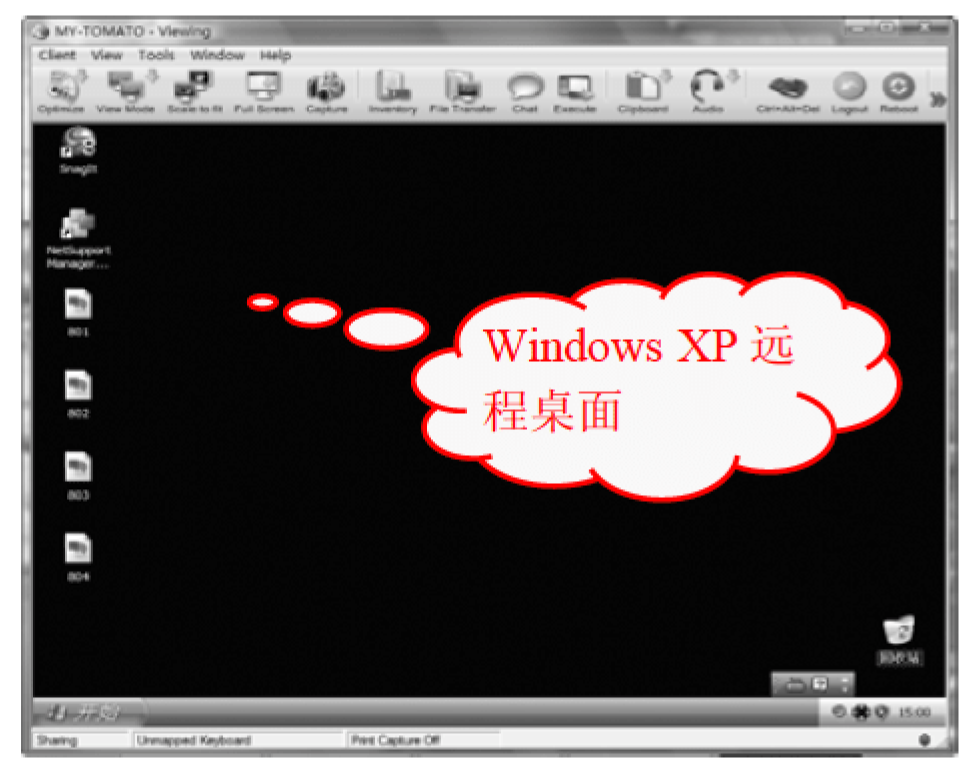












注　意　事　项

快速连接的时候可以选择用计算机名、用户名或者是 IP 地址。

(3) 控制界面功能

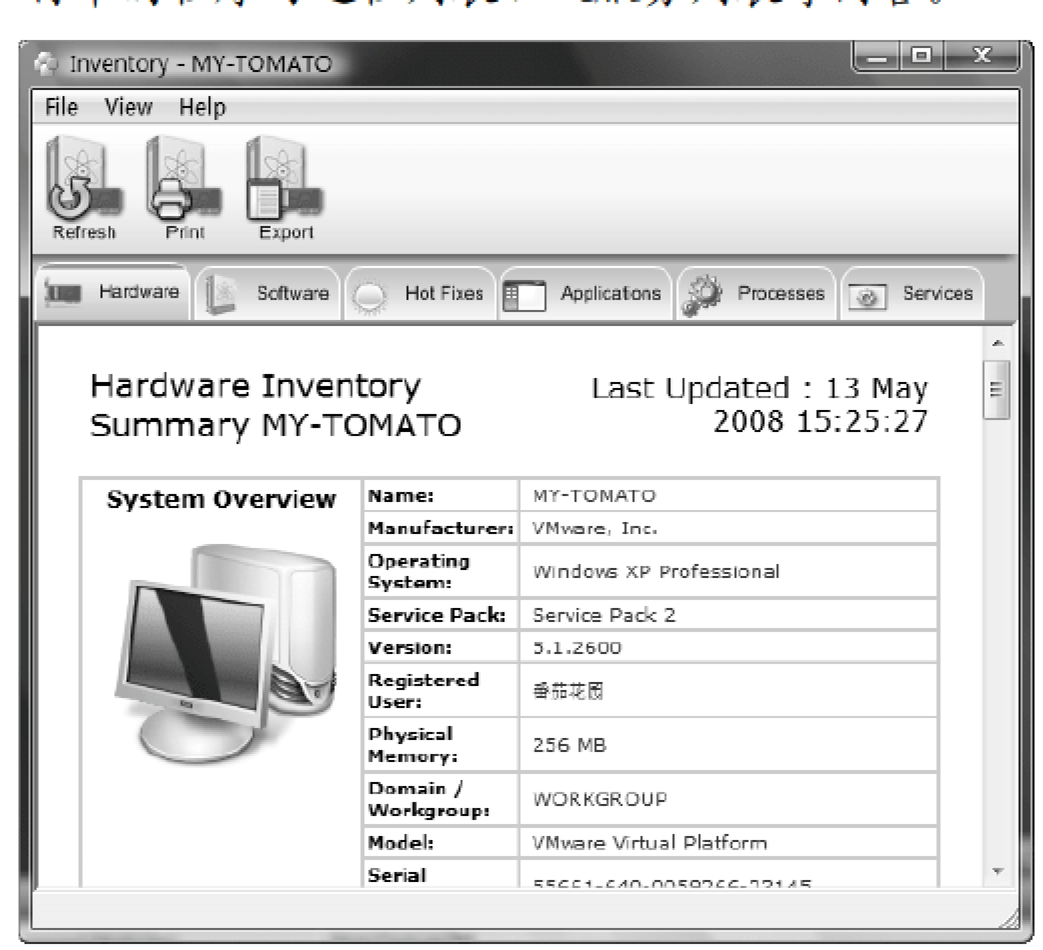
View Mode(视图模式)：选择客户端(被控制端)的浏览

模式。有三种视图模式：Share、Watch 和 Control。

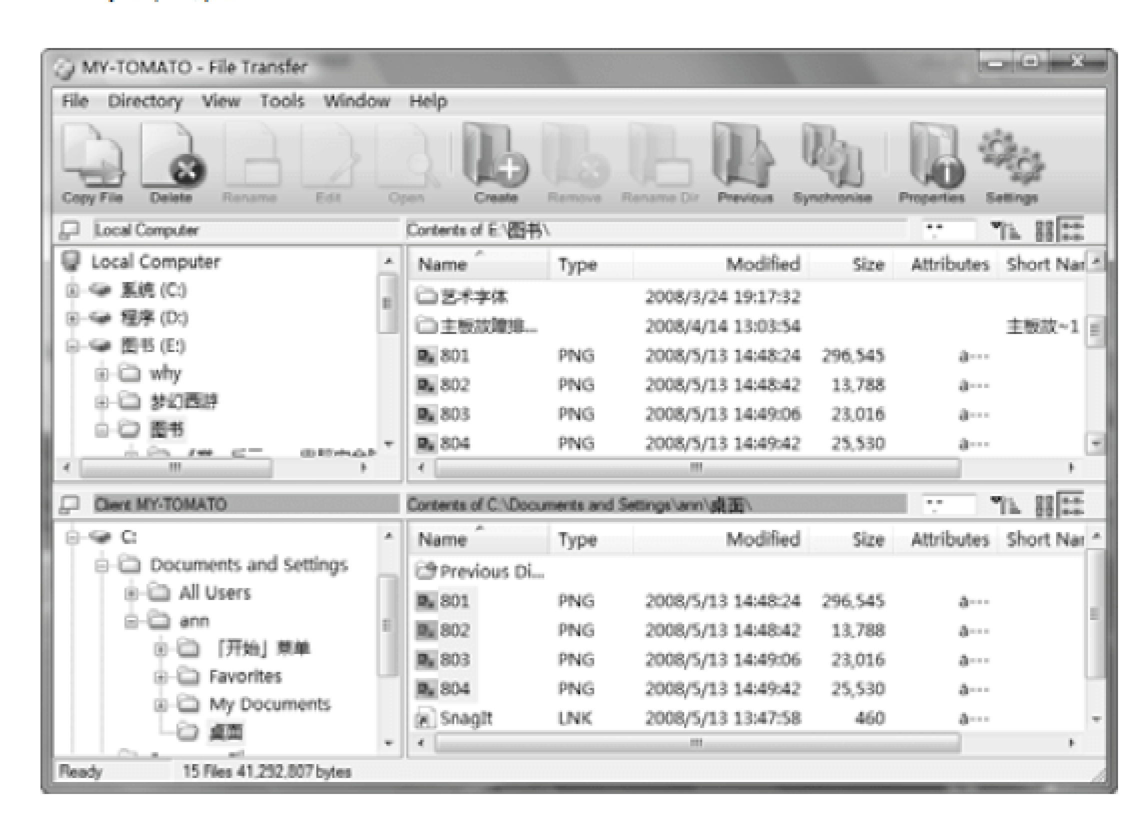
- Share 模式：鼠标和键盘是共享的。
- Watch 模式：不能进行任何操作。
- Control 模式：禁用客户端的鼠标和键盘。



❶ 单击 Inventory 按钮弹出软硬件信息列表窗口，窗口中包括硬件列表、安装的软件列表、补丁更新列表、运行中的程序与进程列表以及服务列表等内容。



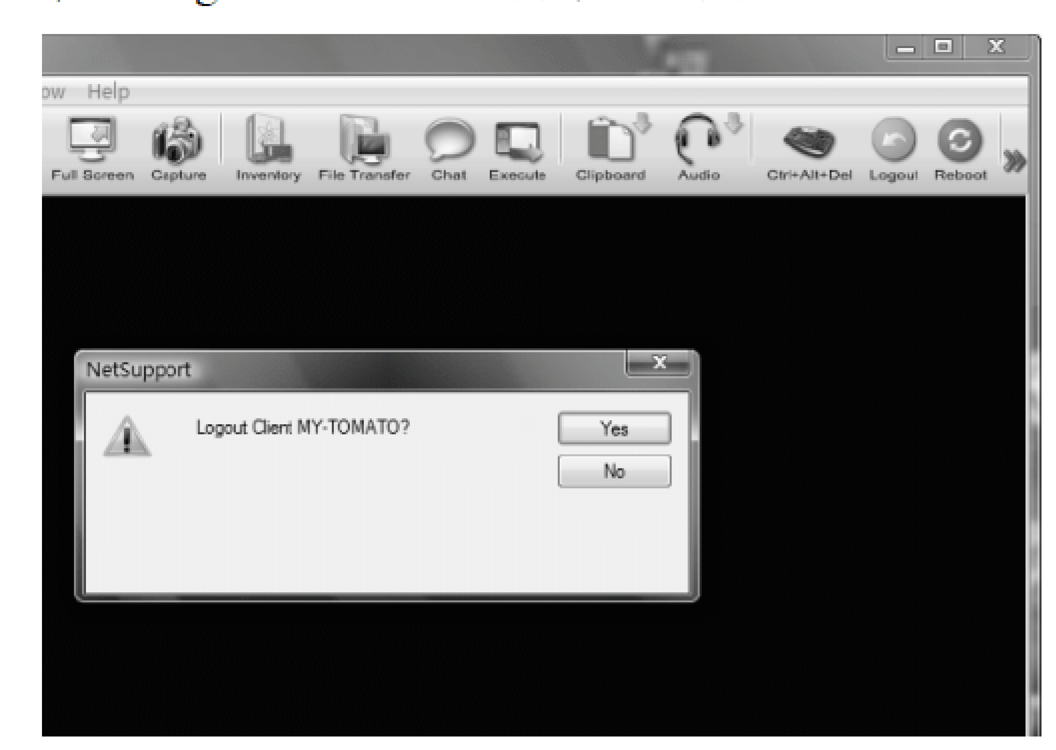
❷ 单击 File Transfer 按钮，在控制端和客户端进行文件的传输。



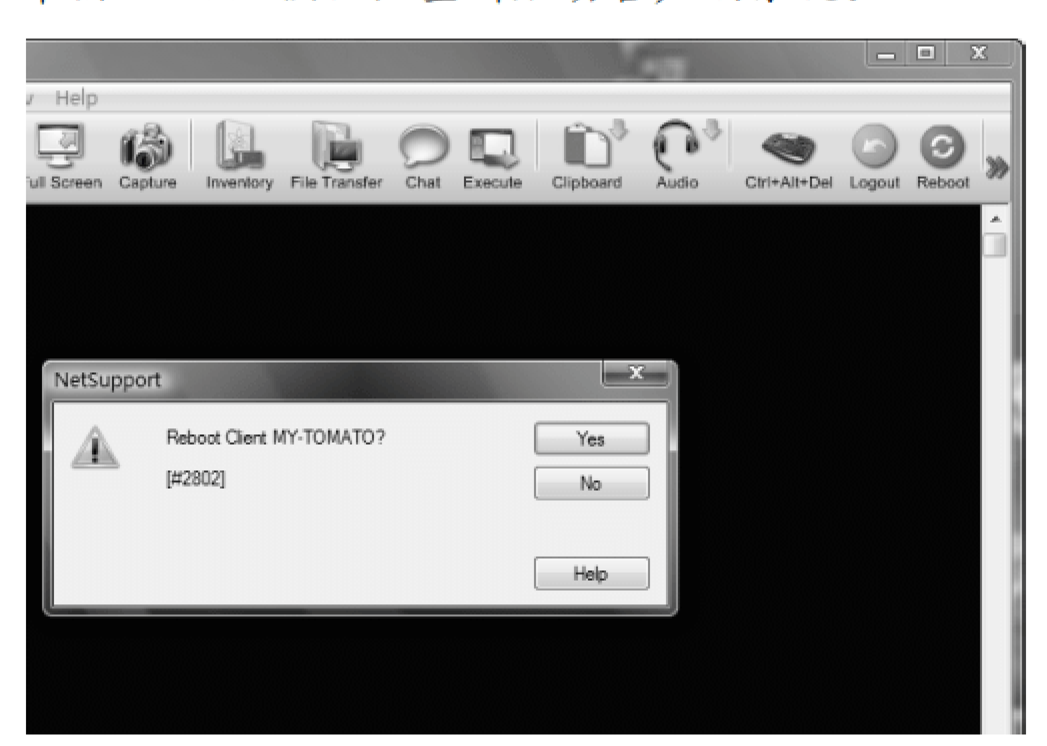
❸ 单击 Chat 按钮，在控制端和客户端进行文字聊天。



❹ 单击 Logout 按钮，注销客户端的系统。



❺ 单击 Reboot 按钮，重新启动客户端系统。



注　意　事　项

如果客户端的 IP 地址或者用户名被不法分子获得，系统就很容易被控制。

技巧225　使用 Super Silent Manager 进行远程监视

Super Silent Manager 是一个操作简单的远程监视工具，可以通过麦克风和摄像头对远程终端进行监视。

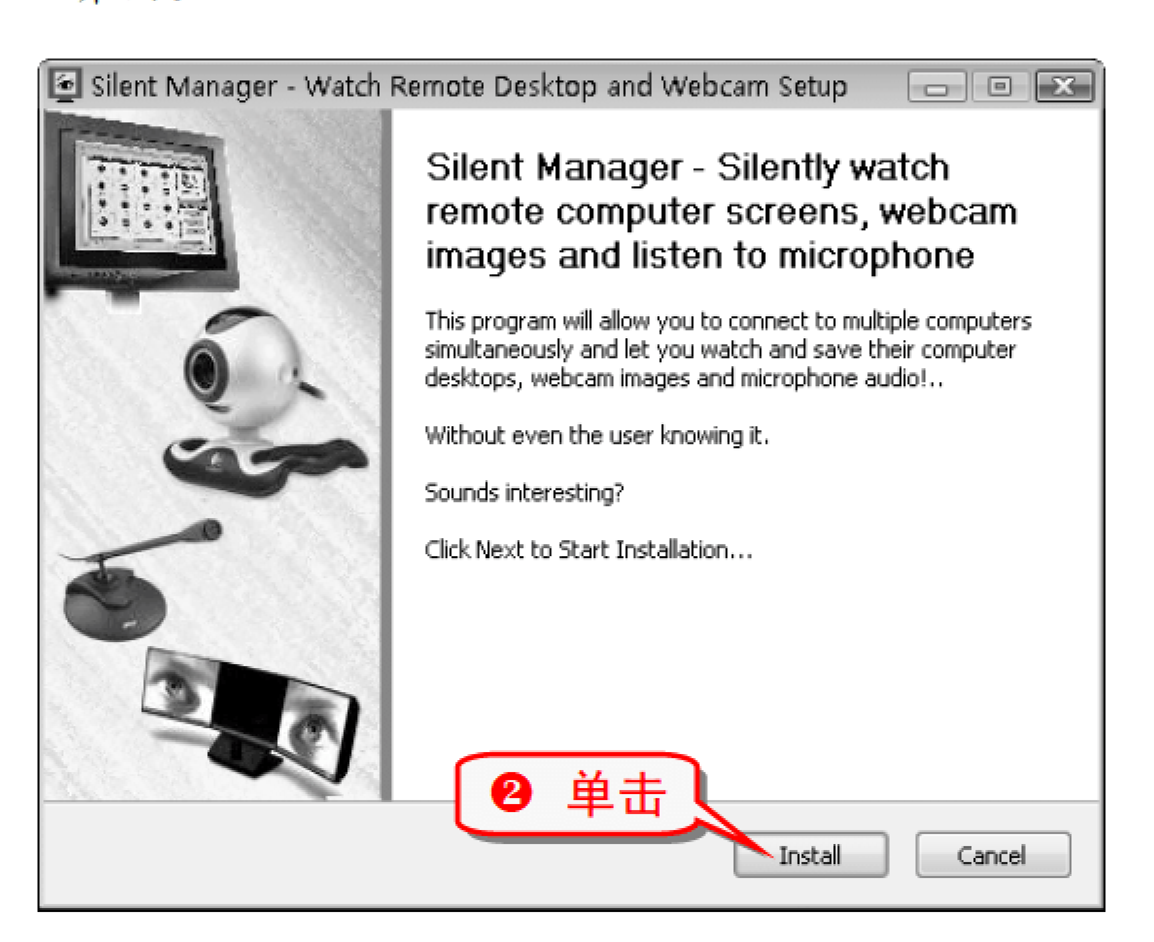
要使用 Super Silent Manager 进行监视，必须在远程终端安装一个 Super Silent Client 程序，在监视端要安装一个 Super Silent Manager 程序。

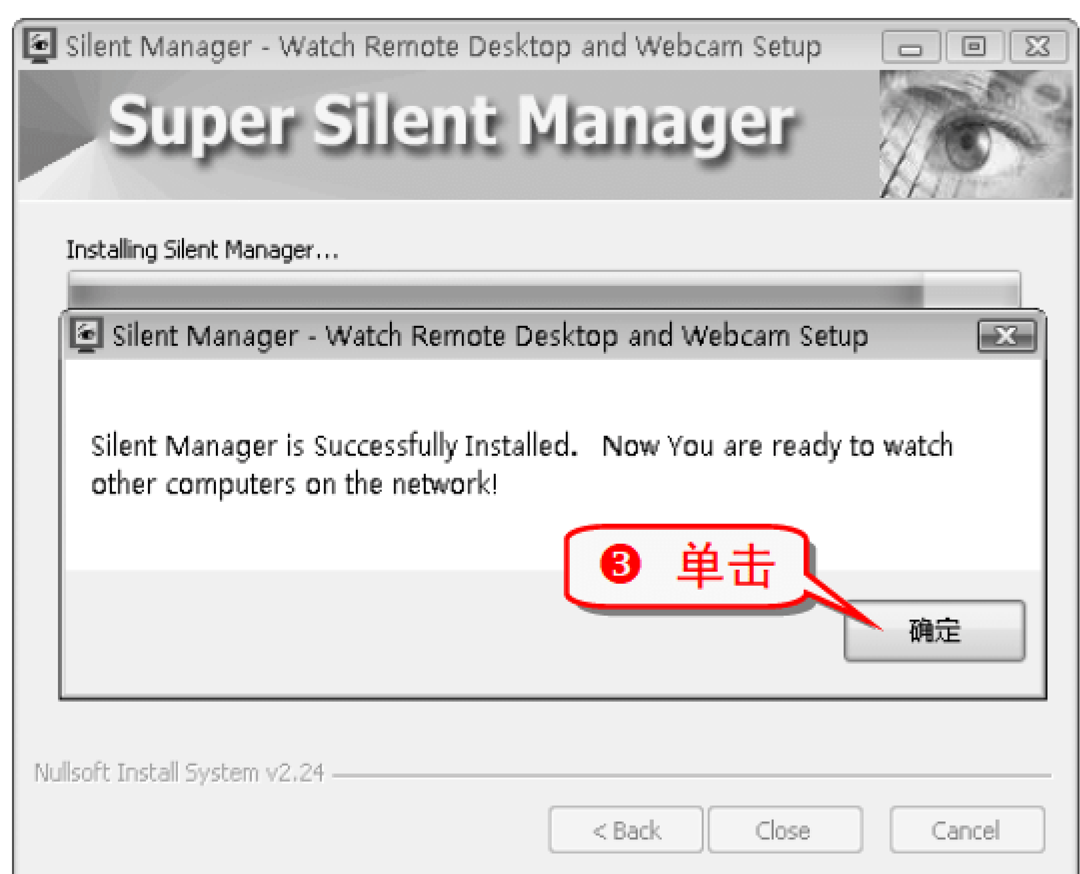


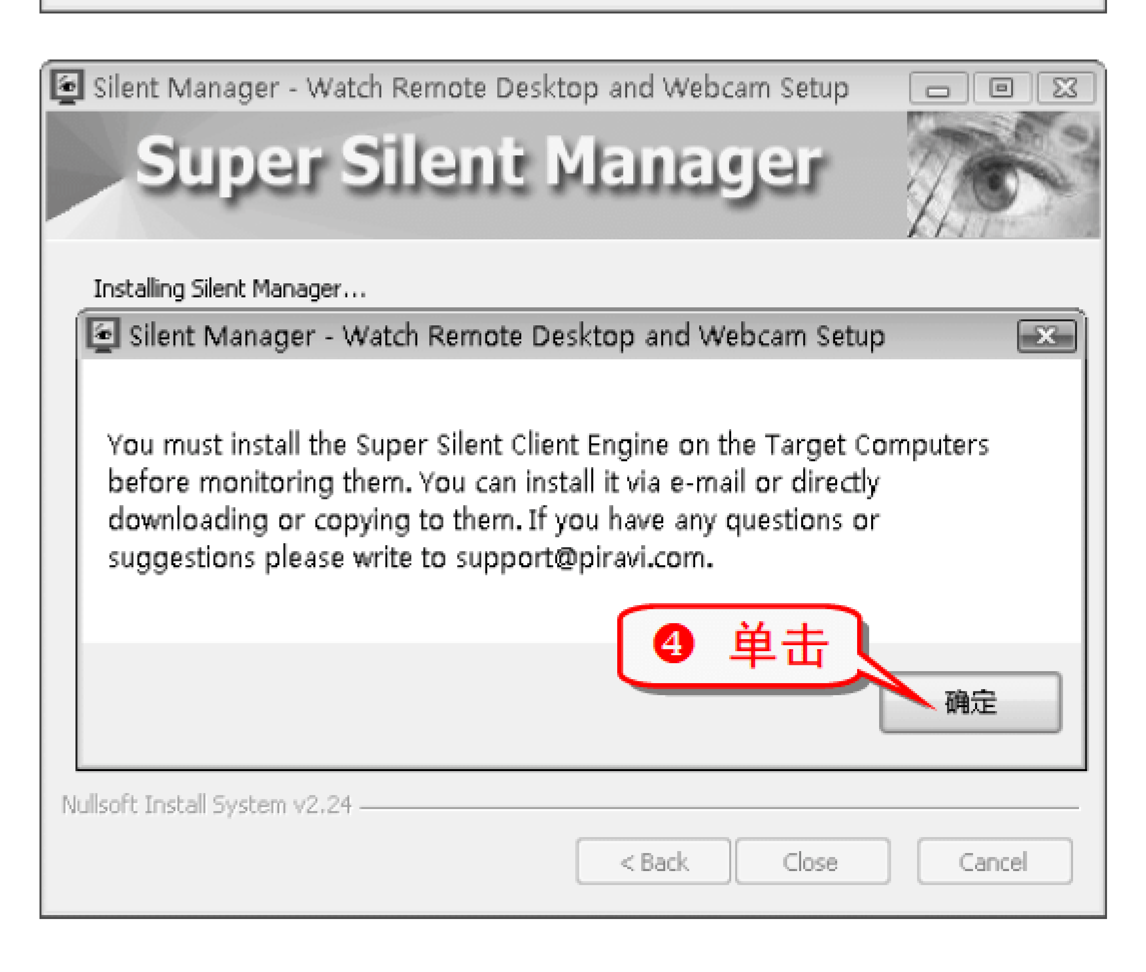
(1) 安装 Super Silent Manager

想要通过当前电脑监视远程电脑，必须把 Super Silent Manager 装在当前电脑上。

❶ 双击 Super Silent Manager 的安装软件，进入安装界面。









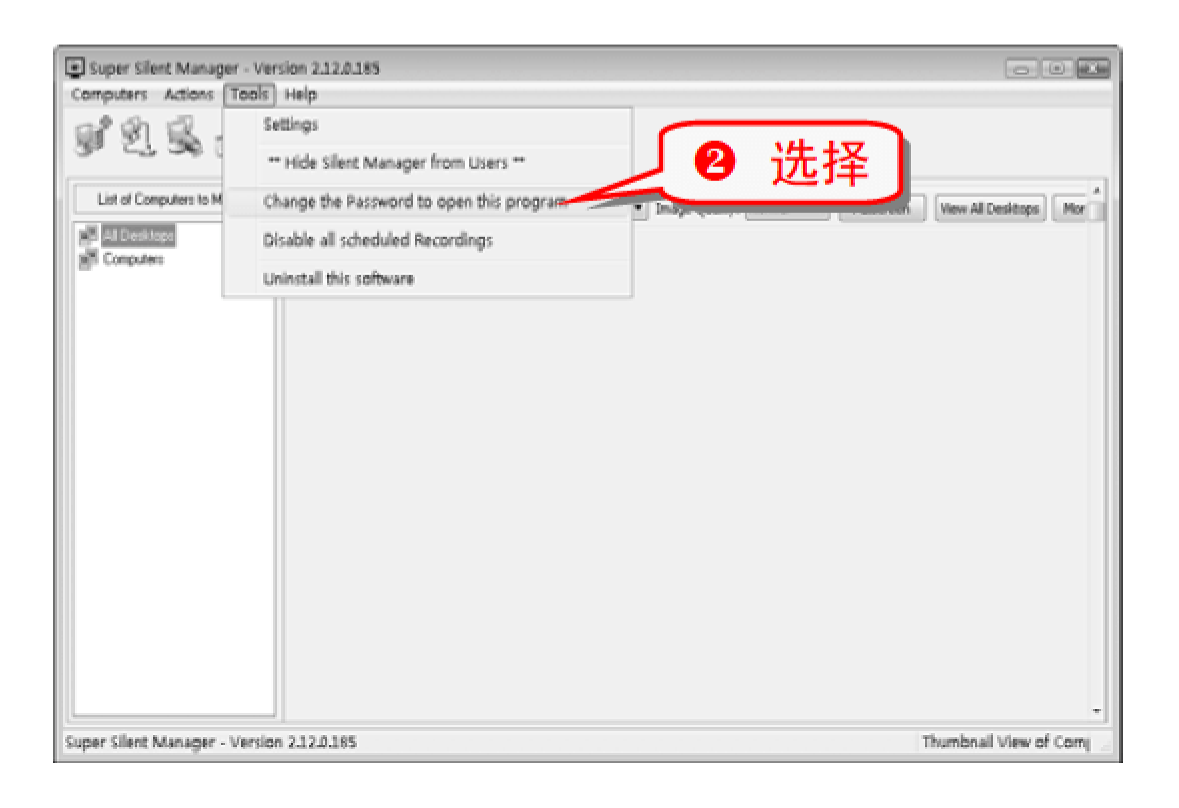
注 意 事 项

在最后一步输入 E-mail 地址的时候，必须填入正确的 E-mail 地址。

(2) 为 Super Silent Manager 设置密码

为了安全起见，可以为 Super Silent Manager 设置一个启动密码，这样每次启动 Super Silent Manager 时就必须要输入密码。

❶ 选择“开始”→“所有程序”→Super Silent Manage 命令，弹出 Super Silent Manage 主程序界面。





❺ 完成上述过程后，再次启动 Super Silent Manage 就会出现如下图所示的对话框，要求输入密码。

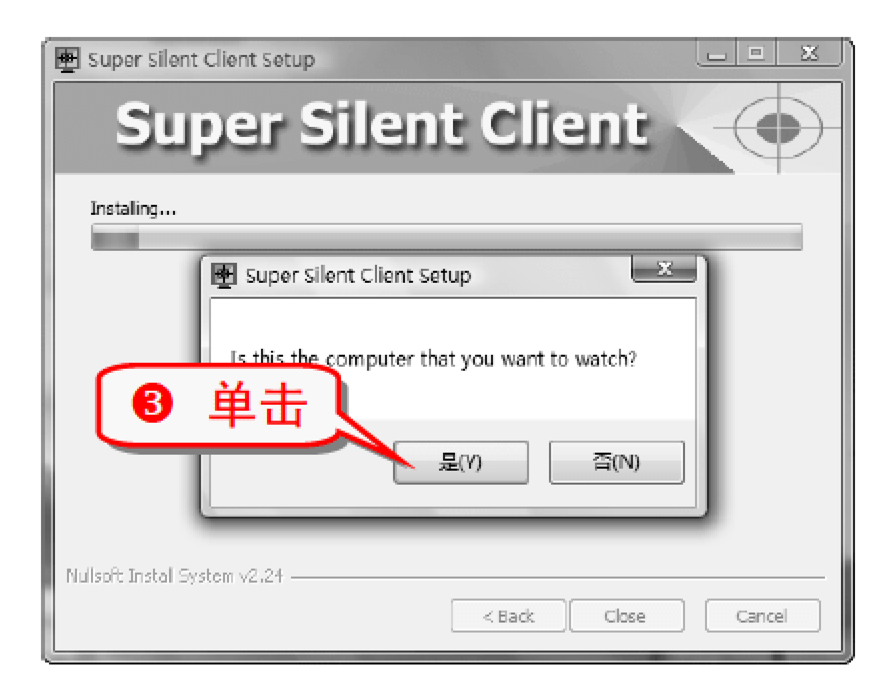


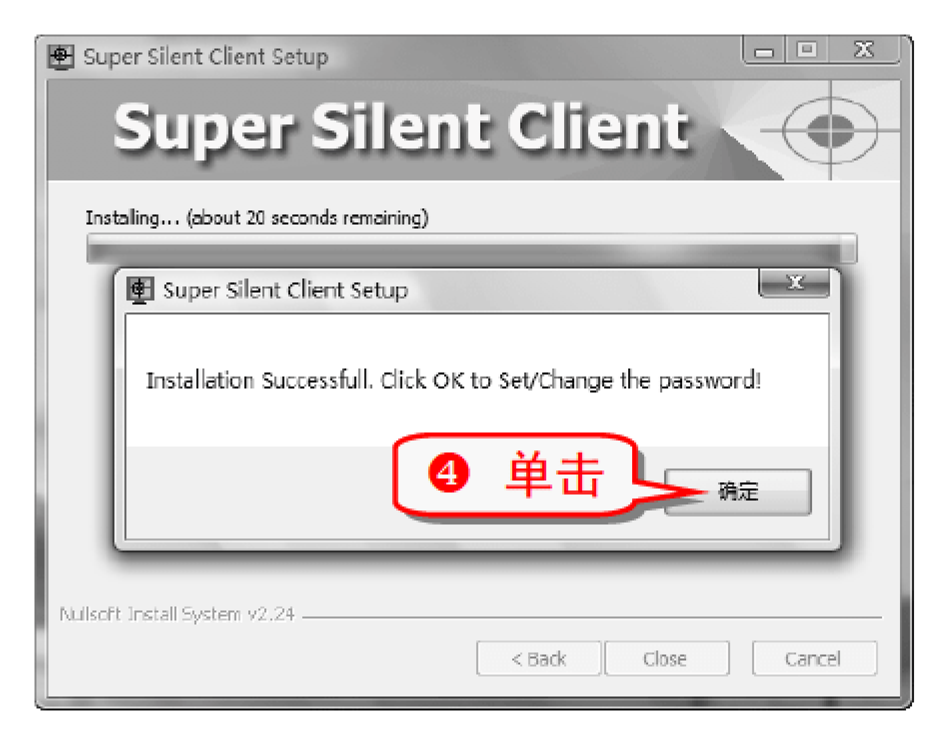
(3) 安装 Super Silent Client

只有在远程客户端上安装了 Super Silent Client，才能利用 Super Silent Manager 对其进行监视。

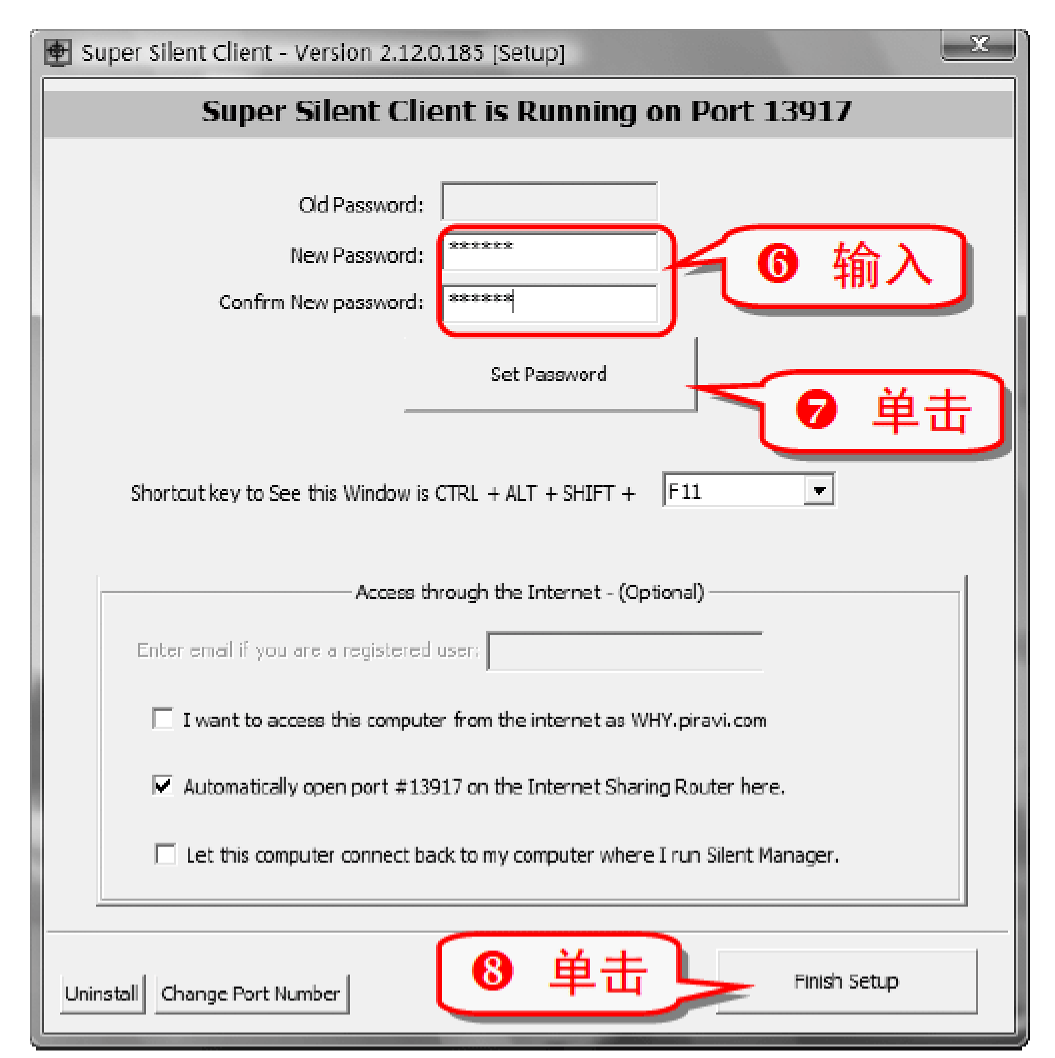
❶ 双击 Super Silent Client 的安装软件，进入安装界面。

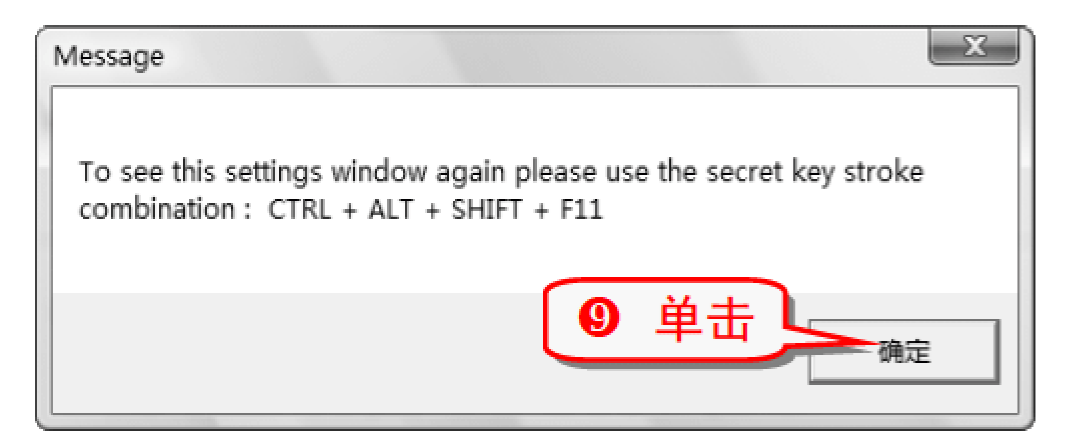












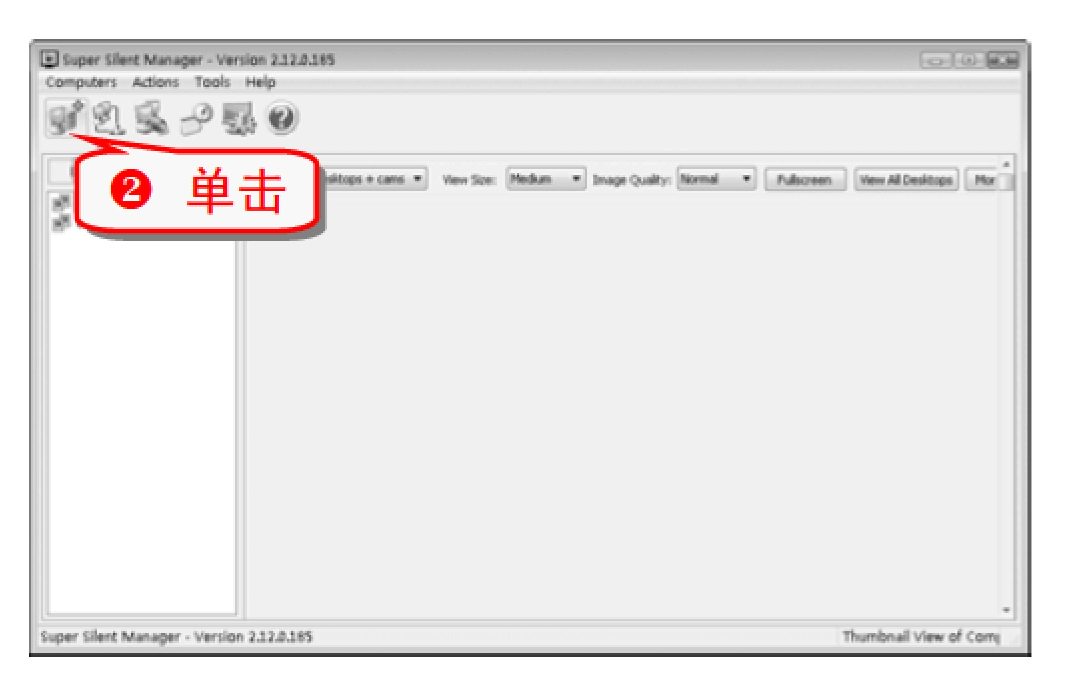


在安装 Super Silent Client 的时候必须要为其设置密码。

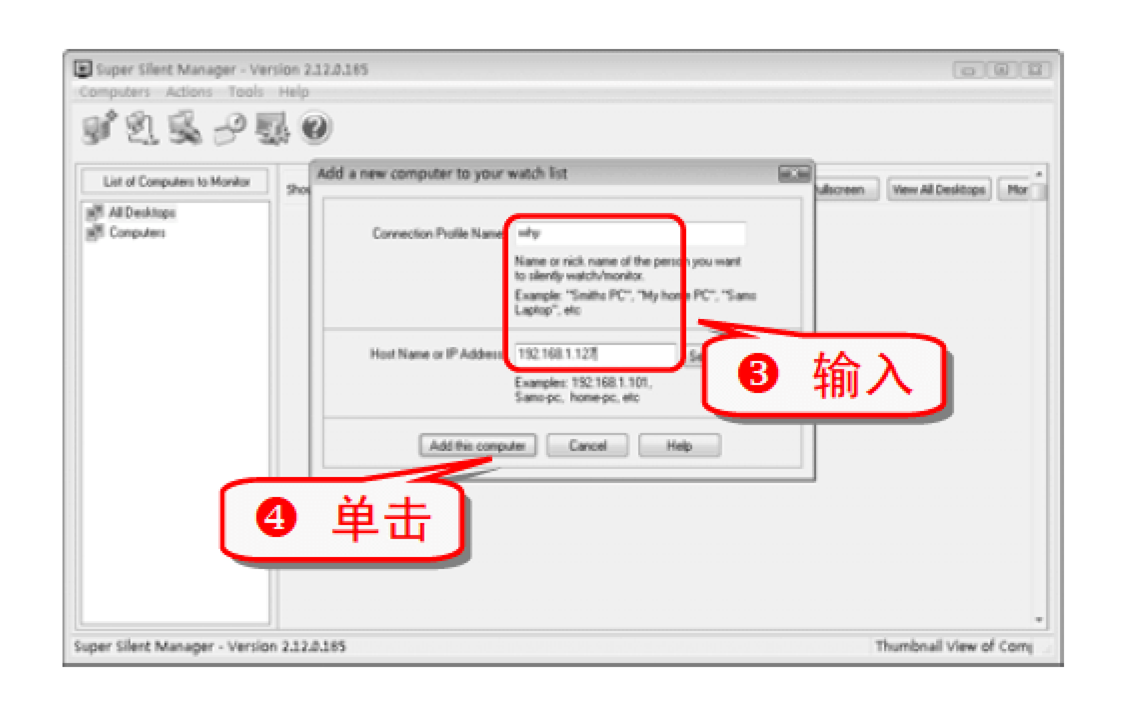
(4) 连接远程电脑

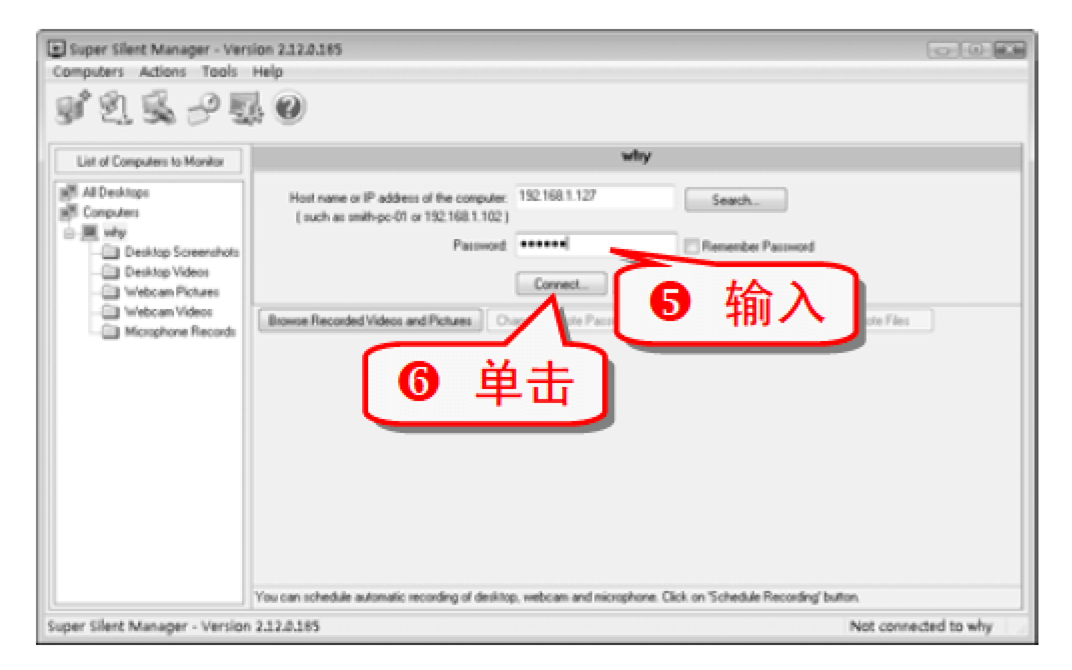
都安装好以后就可以进行远程监视的相关设置了。

❶ 运行 Super Silent Manager，打开程序主界面。

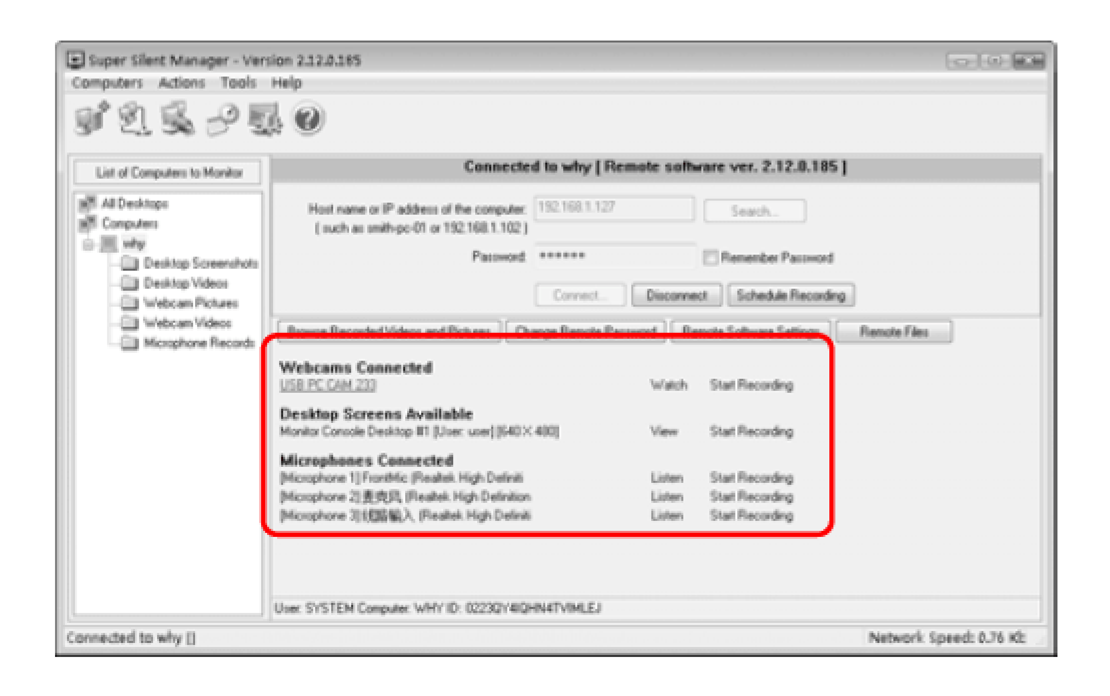






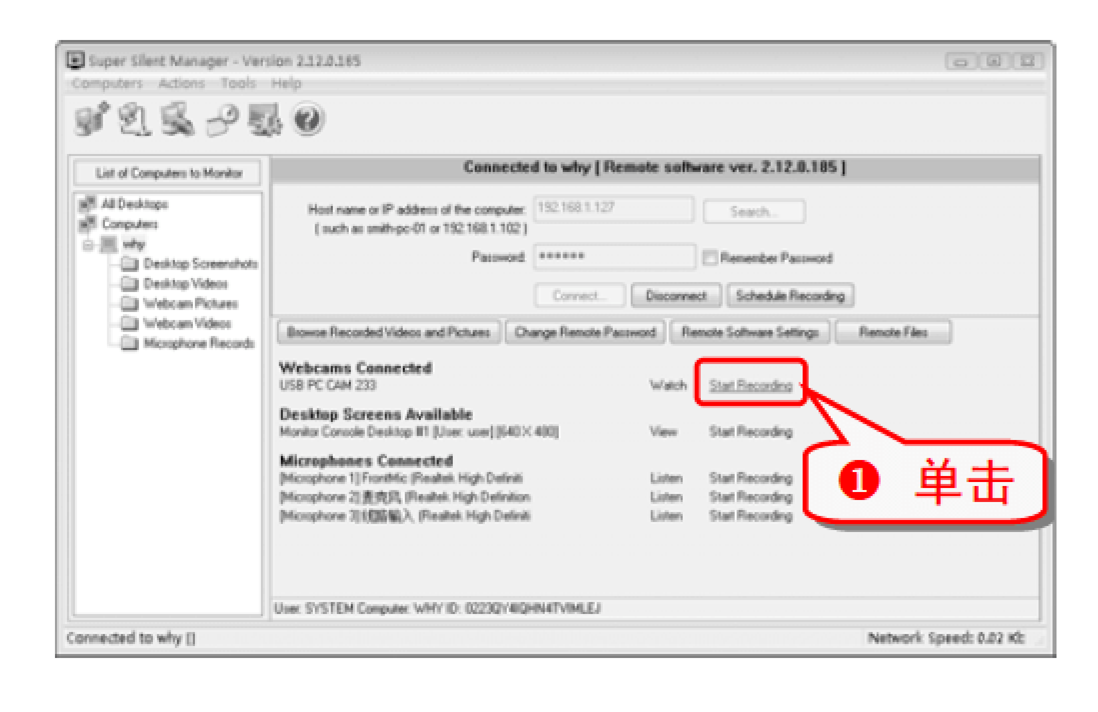


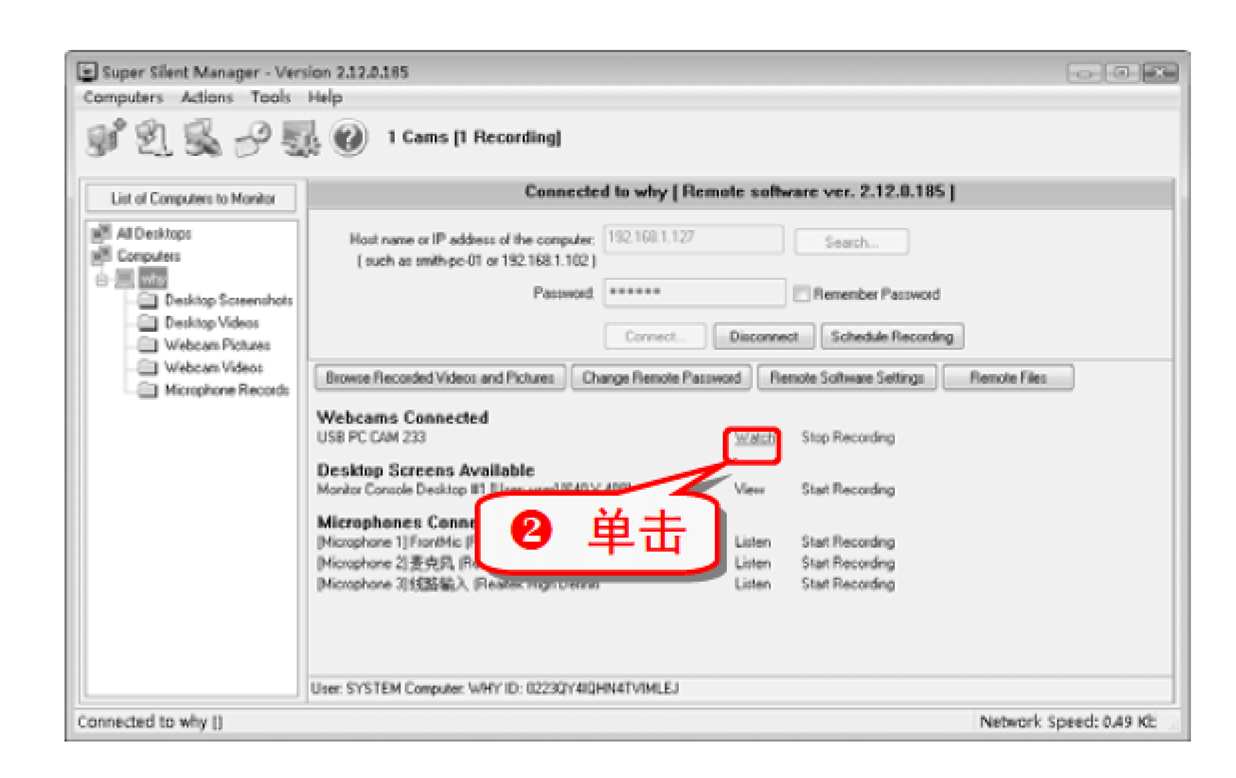
❼ 连接成功后在窗口中列出可以进行监视或监听的设备。

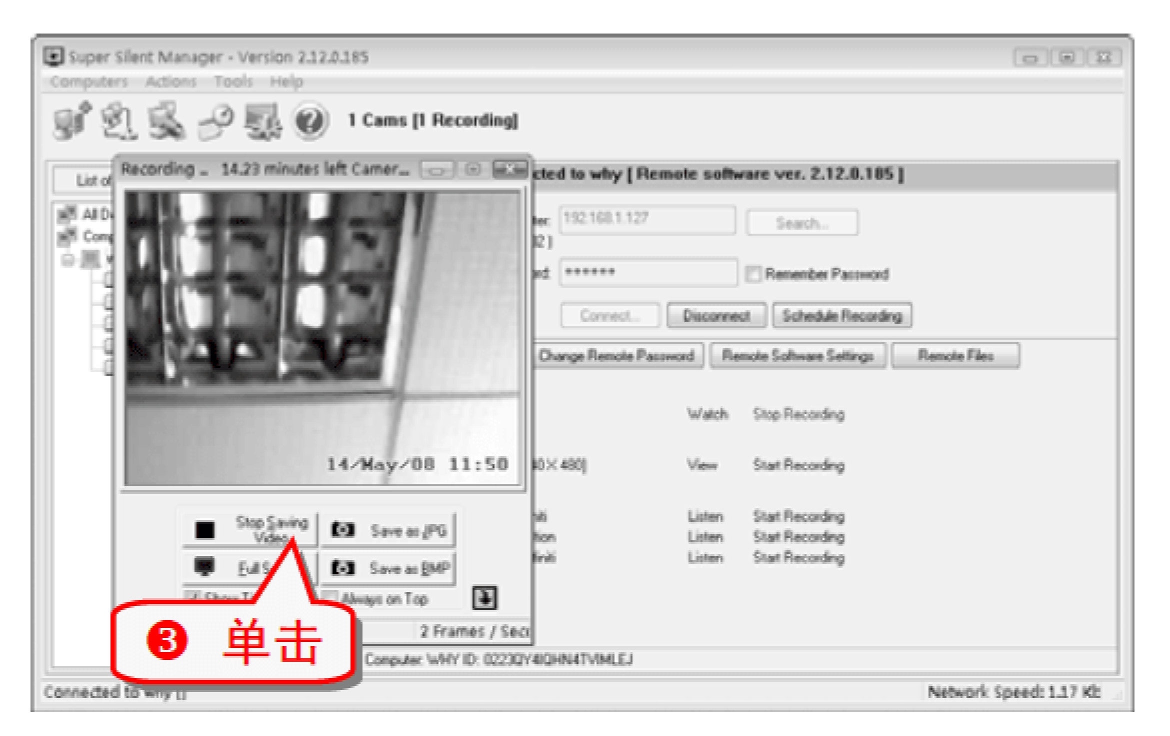


(5) 远程监控

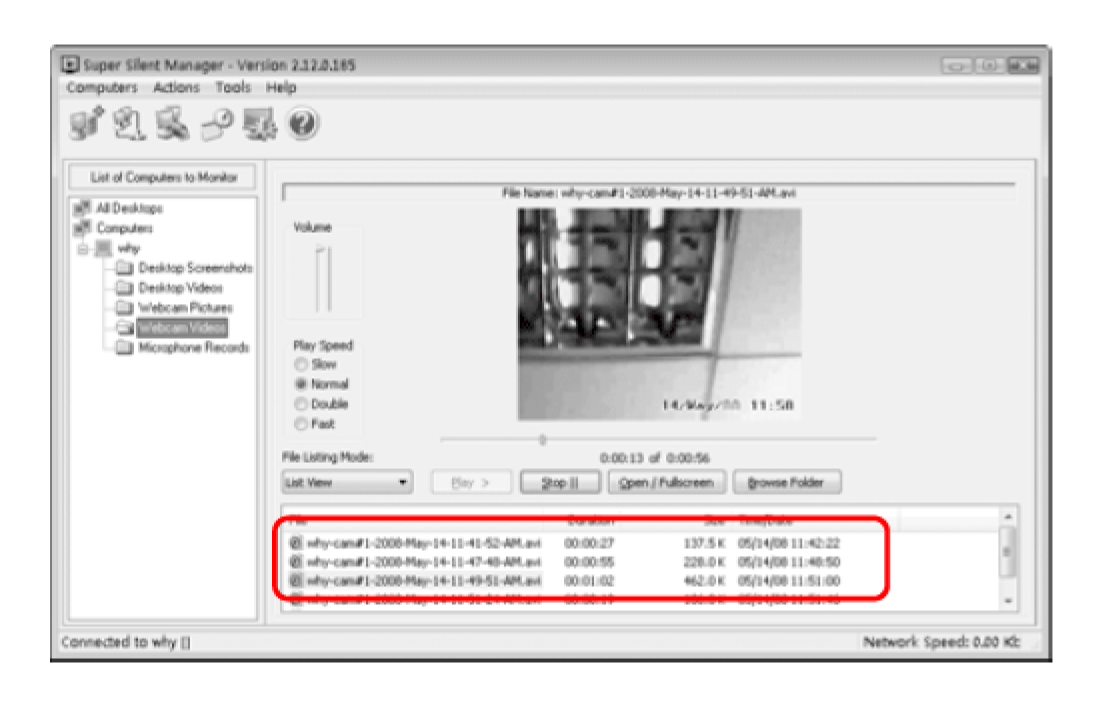
连接成功以后就可以对远程终端进行监视了，下面介绍怎样开启远程终端的摄像头进行监视。

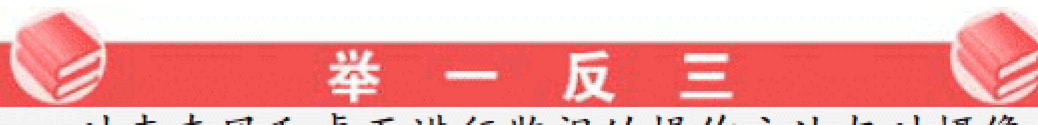






❹ 在该界面下的 WebcamVideos 文件夹中找到摄像头录制的视频。





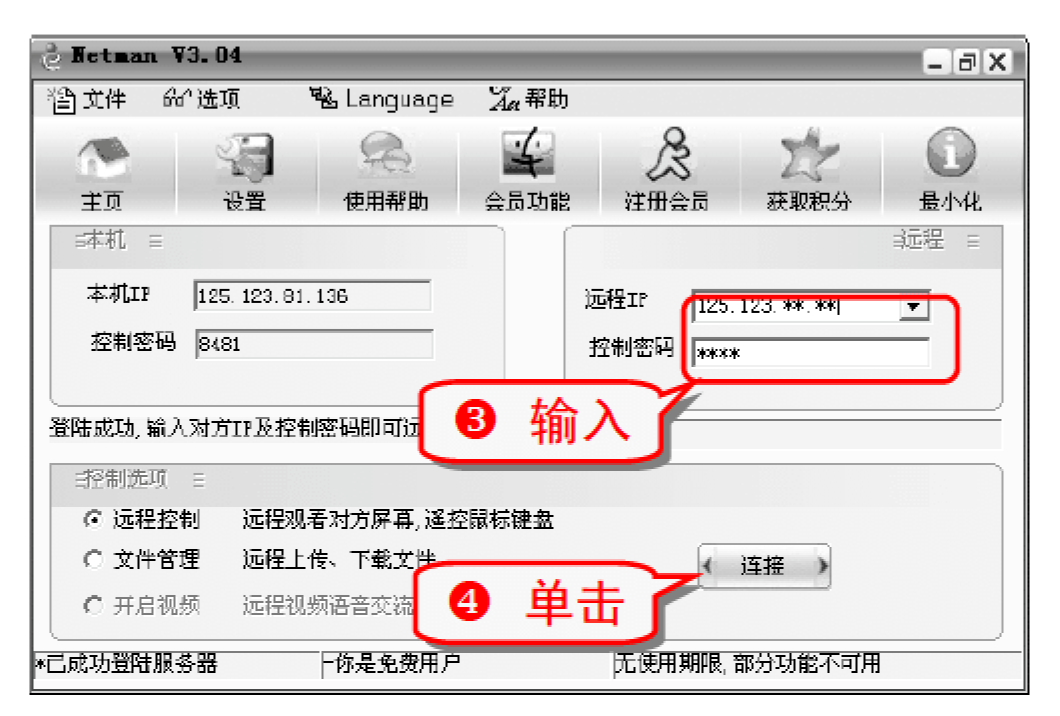
对麦克风和桌面进行监视的操作方法与对摄像头进行监视的操作方法类似。

技巧226　利用 Netman 实现远程控制

Netman(网络人)是一款超级安全的远程控制软件，操作过程简单而且免费使用。

❶ 在控制和被控制的电脑上都装上 Netman 软件。

❷ 获得被控电脑的 IP 和控制密码。



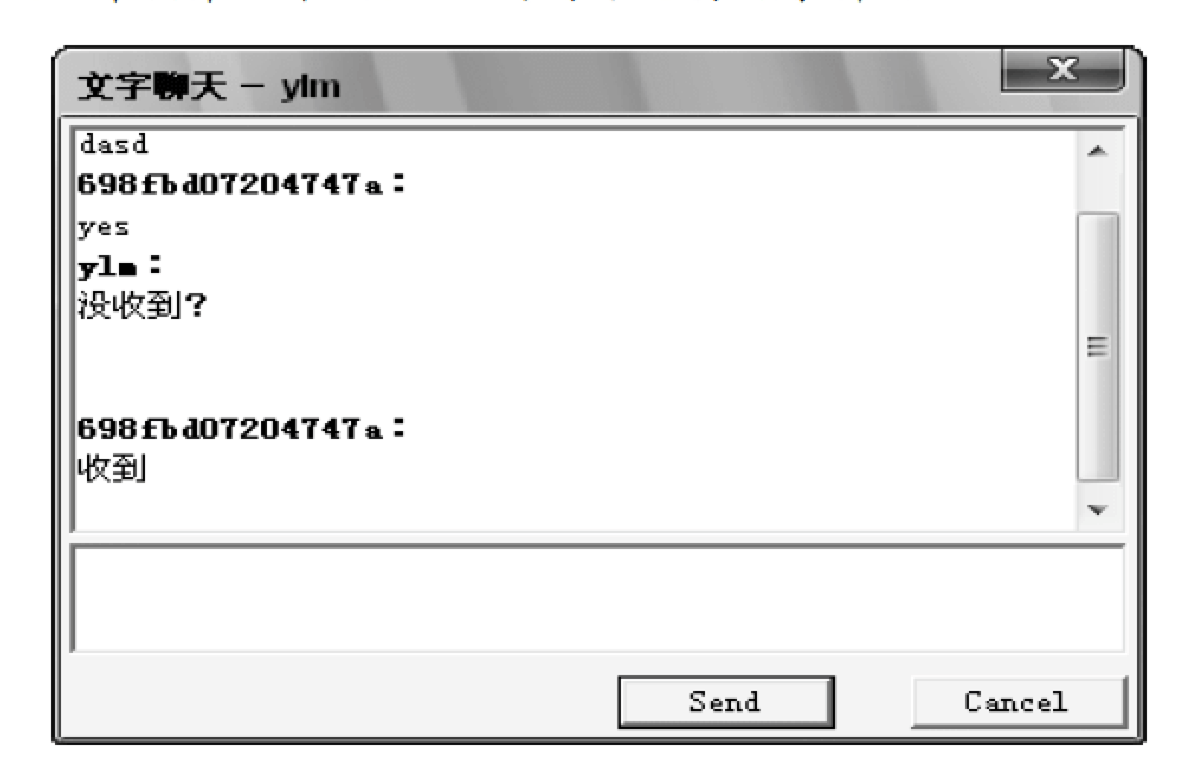
❺ 在桌面上会出现显示对方桌面的一个窗口。



❻ 被控制的一方会在桌面的右下角出现一个如下图所示的简易窗口。



❼ 单击第二个按钮与对方进行文字聊天。



知 识 补 充

Netman 不能在局域网内进行远程控制，因为局域网内的对外 IP 是统一的。使用 Netman 进行控制必须是在双方都同意的原则下，而且每次重新启动 Netman 后，控制密码都会发生改变。

技巧227 利用 Radmin 3.1 实现远程控制

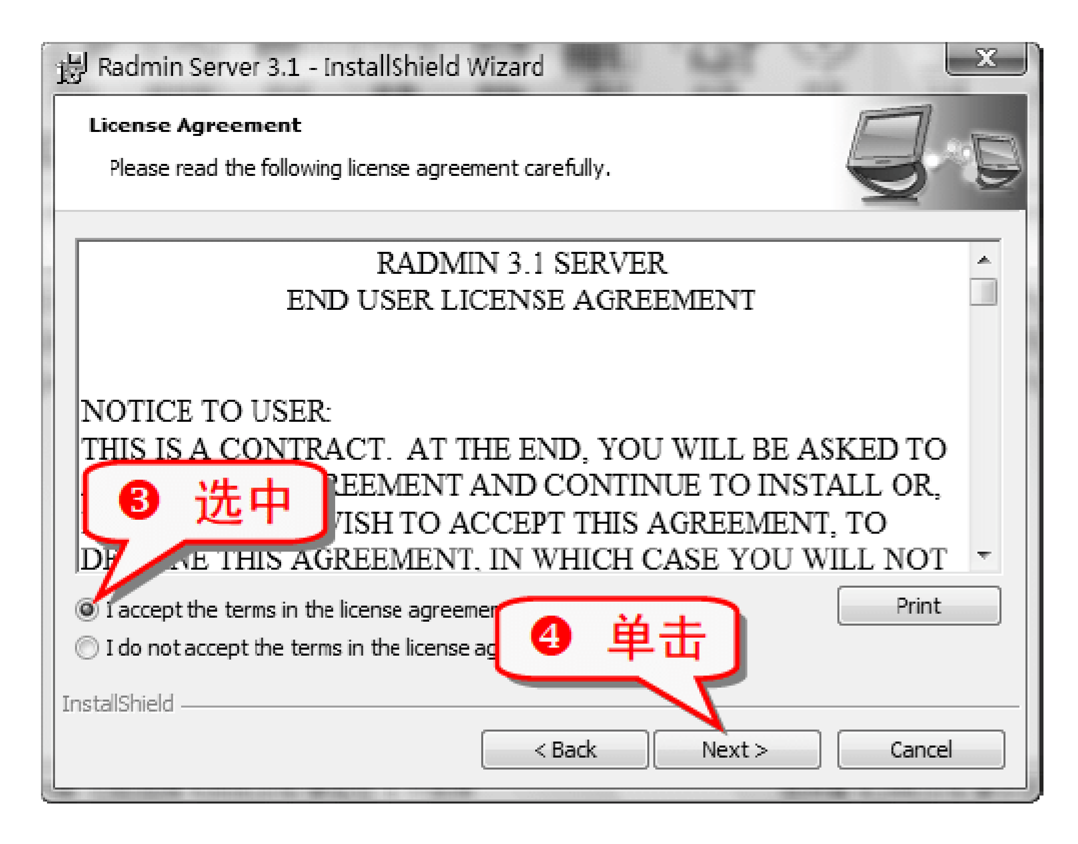
Radmin 3.1 可以远程控制电脑，对其进行完全控制，并且速度很快。

Radmin 3.1 安装包内有服务器端和客户端两个安装软件。安装服务器端，可以使其他电脑访问这台电脑；安装客户端，能通过账号对服务器端进行访问。

(1) 安装服务器端

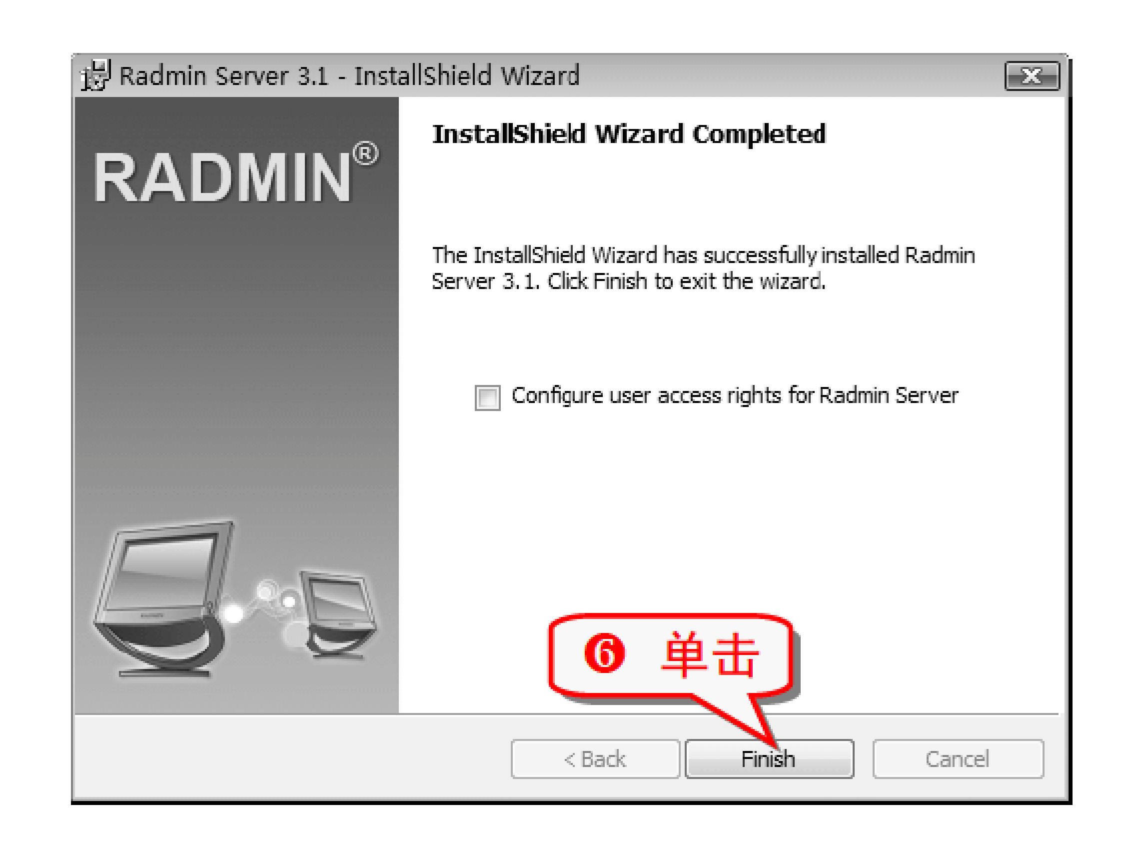
❶ 双击服务器端的安装软件，进入 Radmin Server 的安装界面。

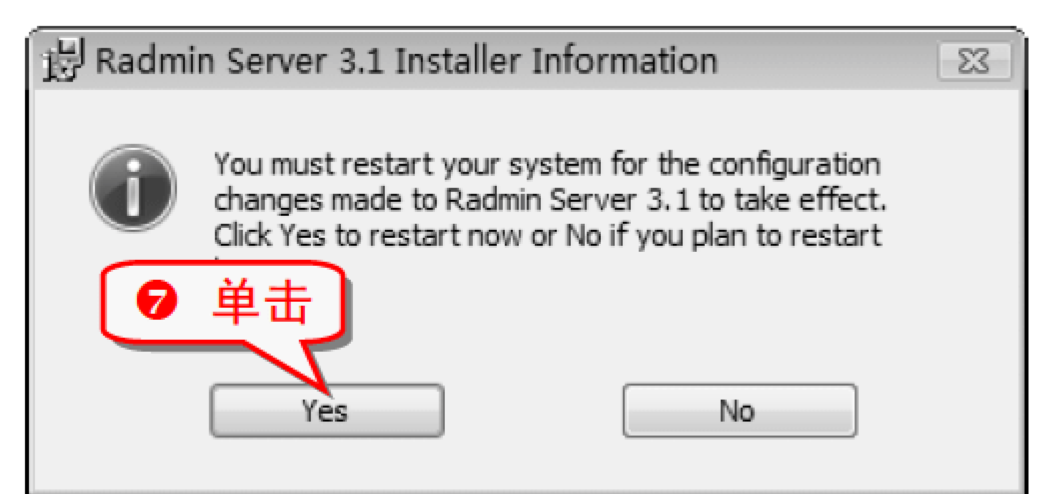










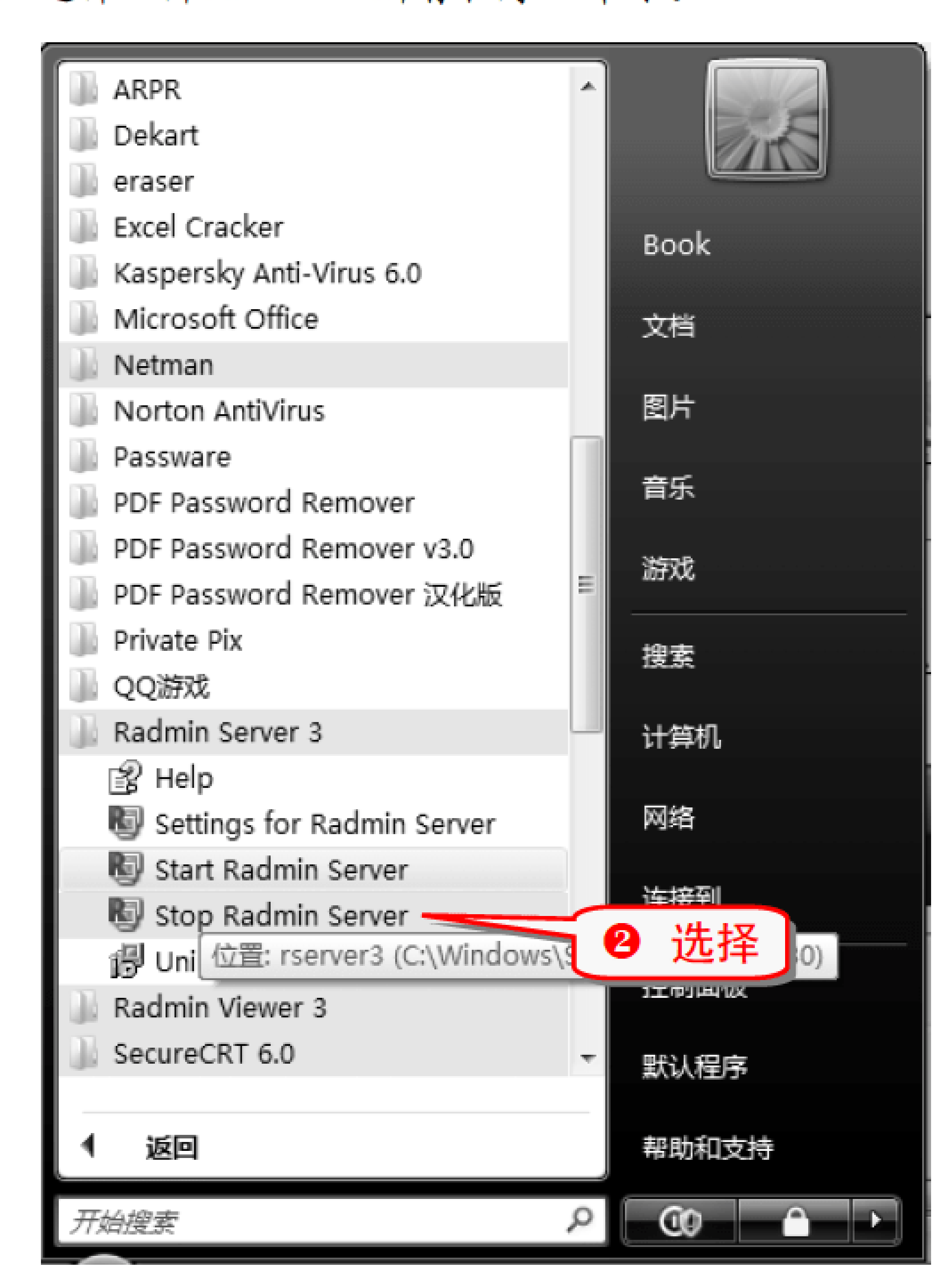




安装好的软件是英文界面，可以根据需要进行汉化。

(2) 配置服务器端

❶ 选择“开始”→“所有程序”命令。











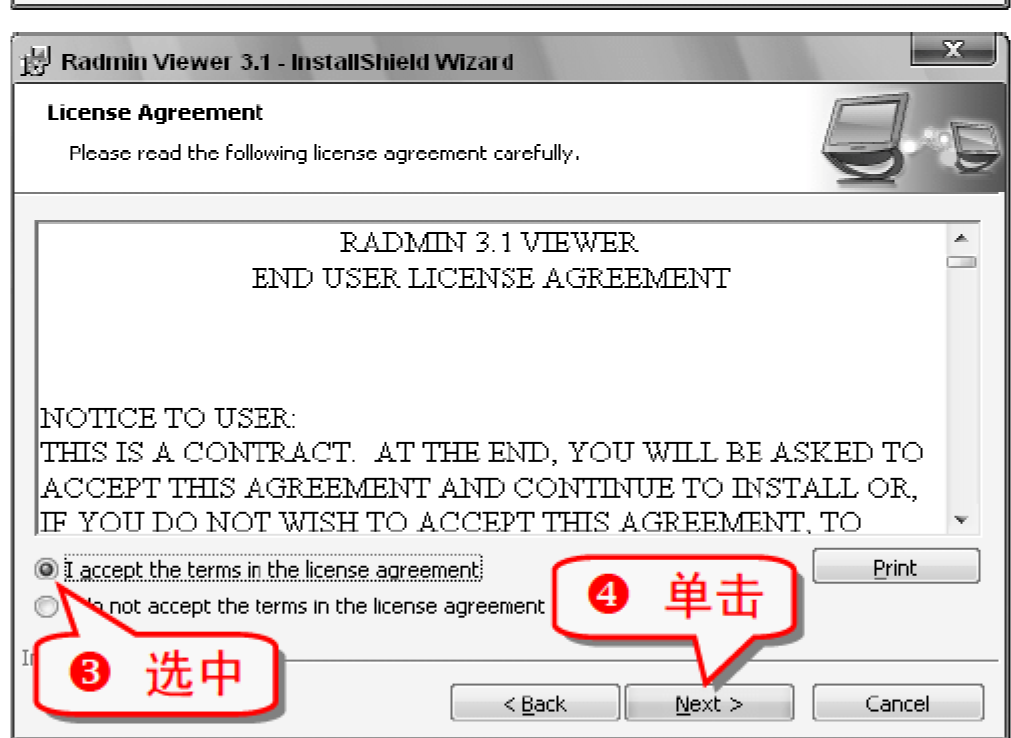


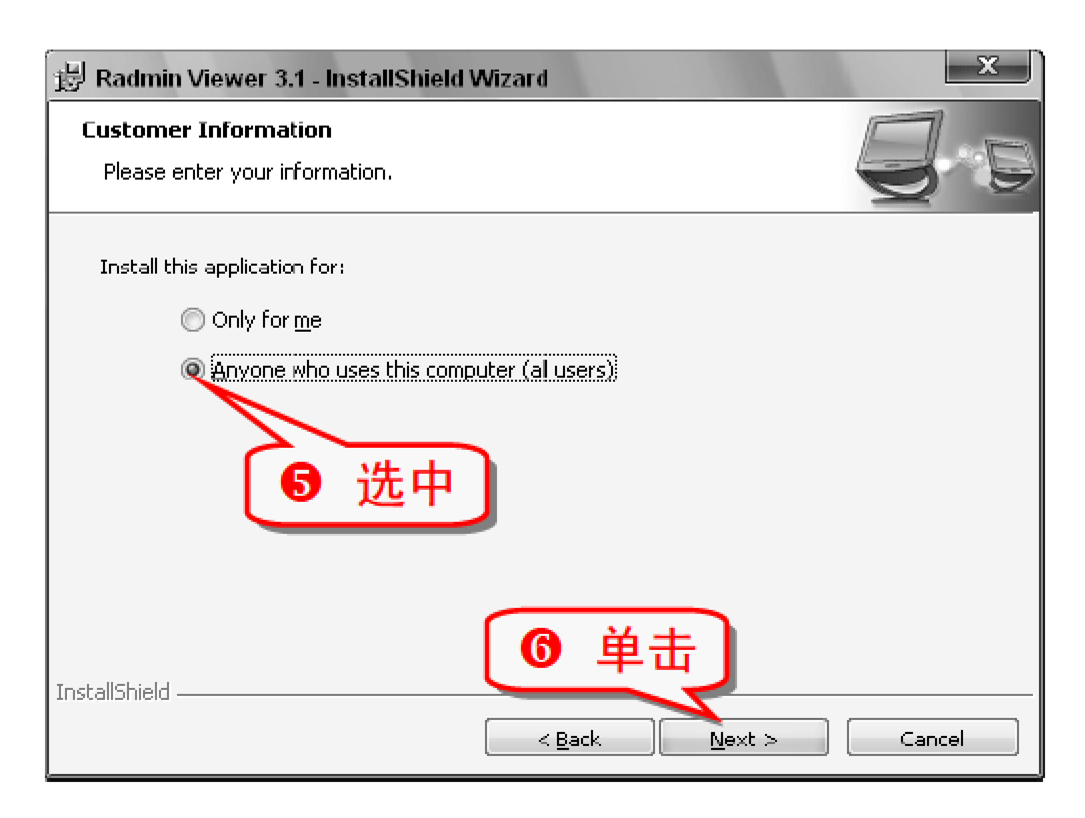


(3) 安装客户端

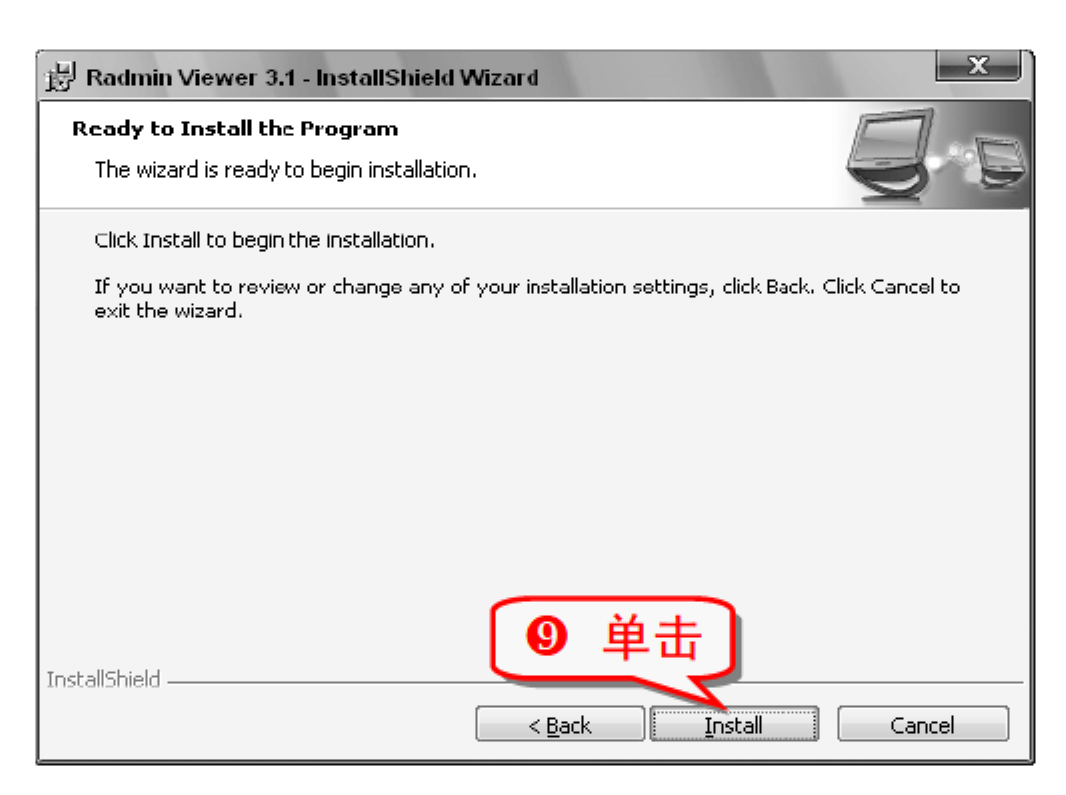
❶ 双击客户端的安装软件，进入 Radmin Viewer 的安装界面。









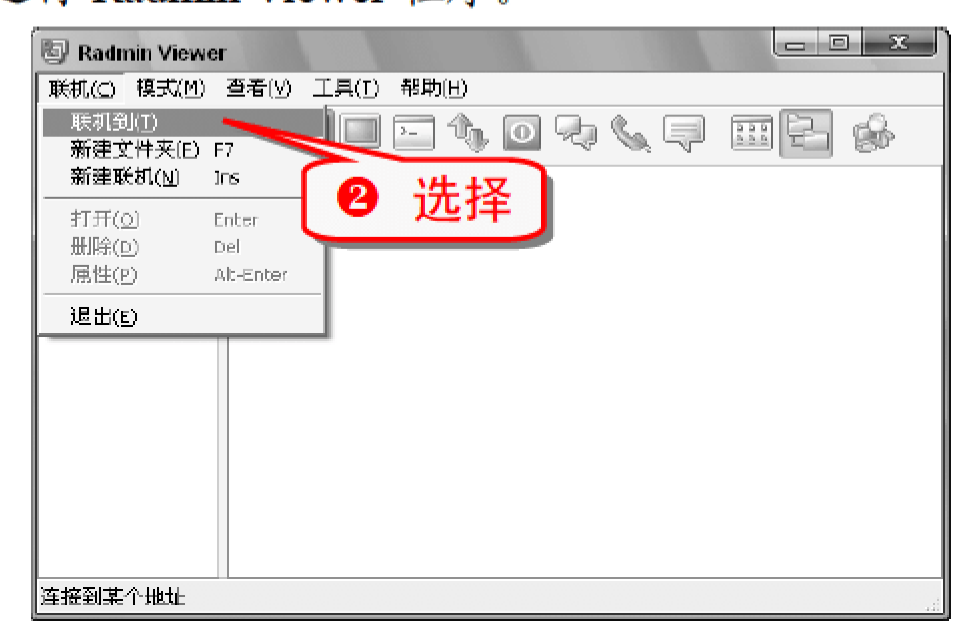


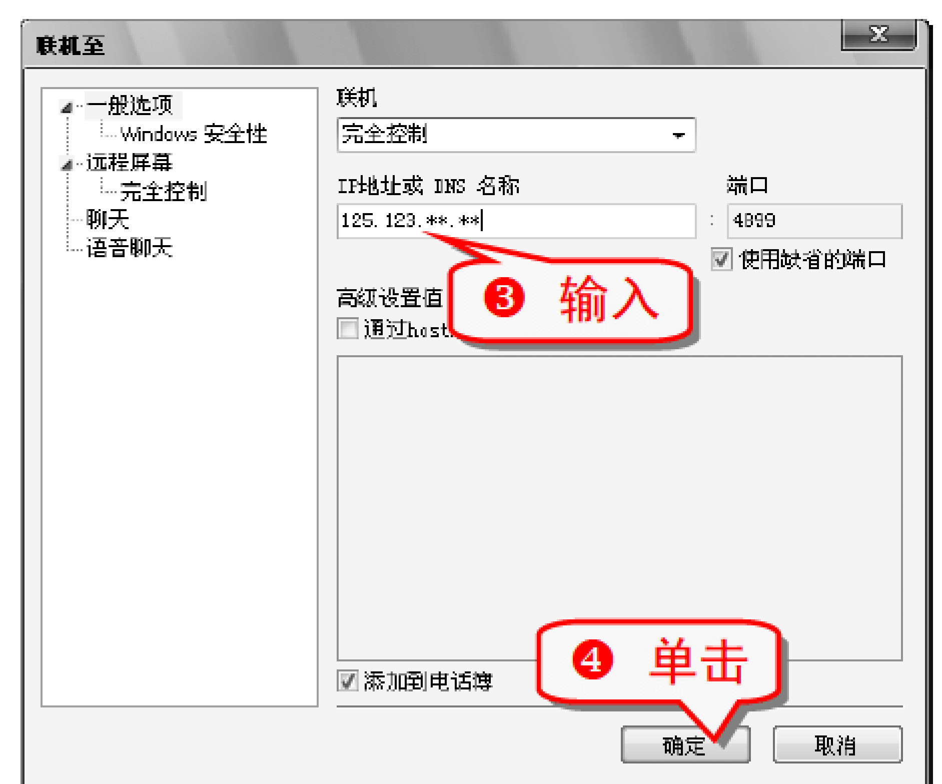




(4) 连接服务器端

❶ 运行 Radmin Viewer 程序。







(5) 进行远程控制

连接服务器端以后会在桌面上显示对方桌面的窗口，并且能对其进行完全控制。



❶ 单击按钮即可弹出文件传送界面，进行相互的文件传送。



❷ 单击按钮即可关闭对方的计算机。



❸ 单击按钮即可进行文字聊天。



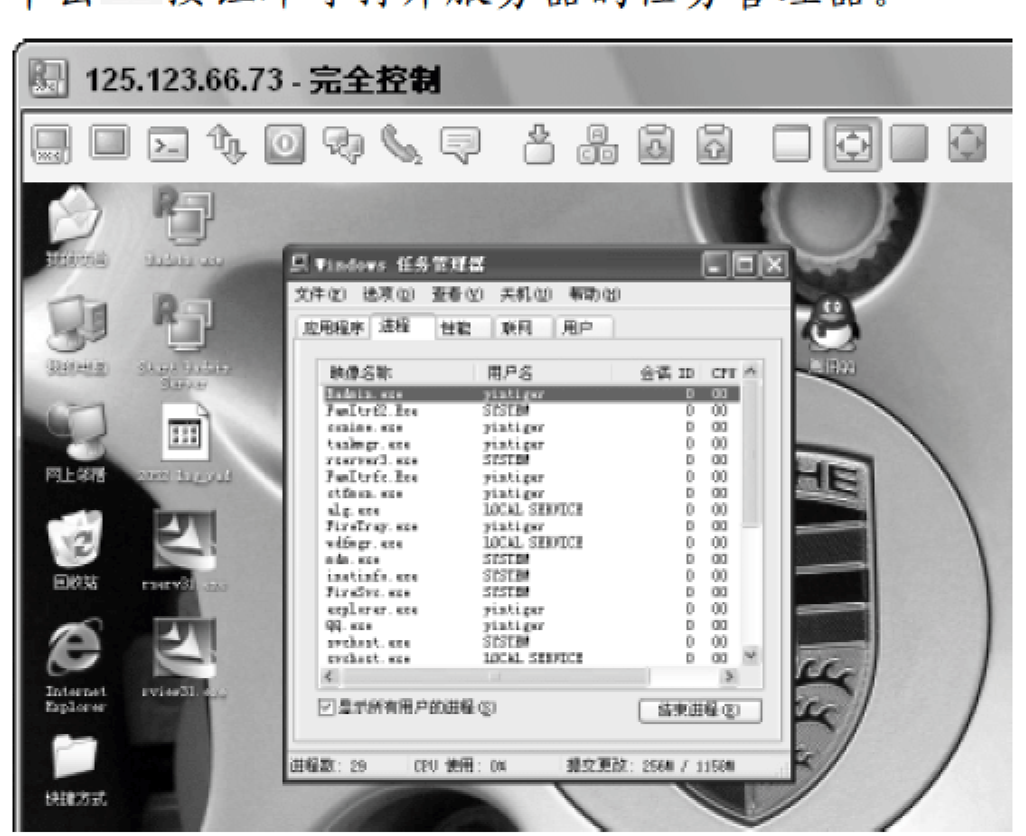


❹ 单击 按钮即可进行语音聊天。





❻ 单击 按钮即可打开服务器的任务管理器。





知 识 补 充

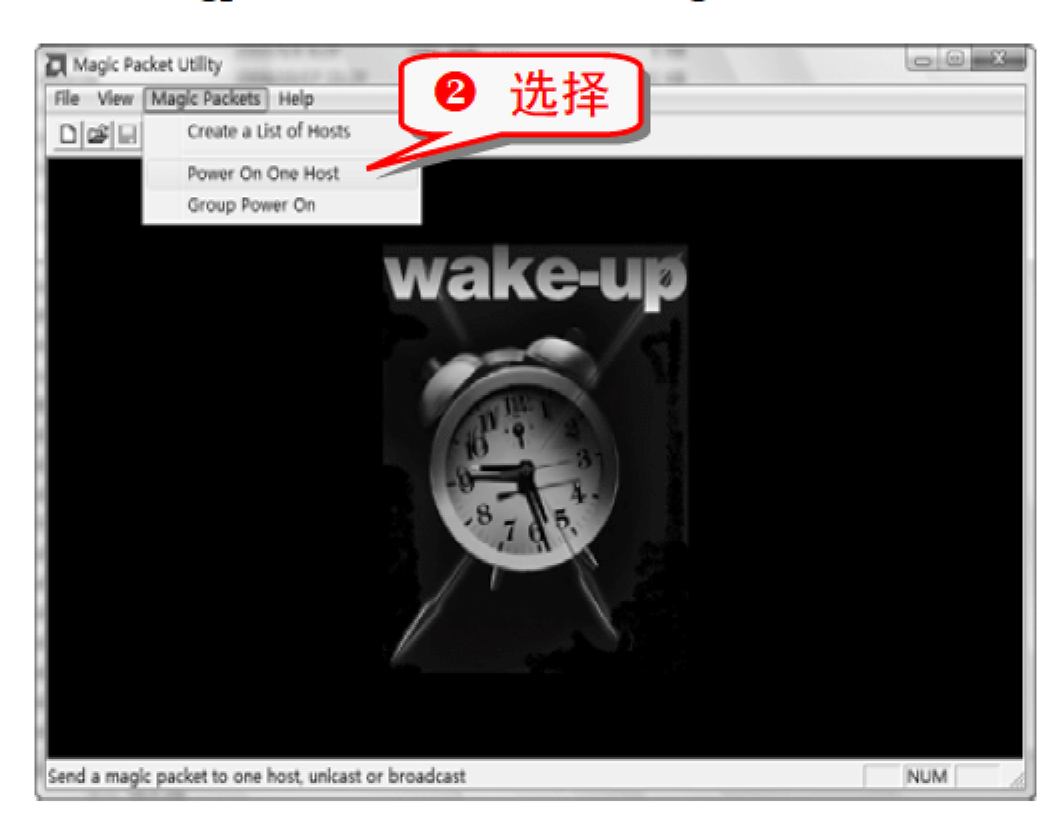
该软件可以在 Windows XP 和 Windows Vista 系统下运行，而且不受局域网和外网的限制。

技巧228 使用 Magic Packet 远程唤醒电脑

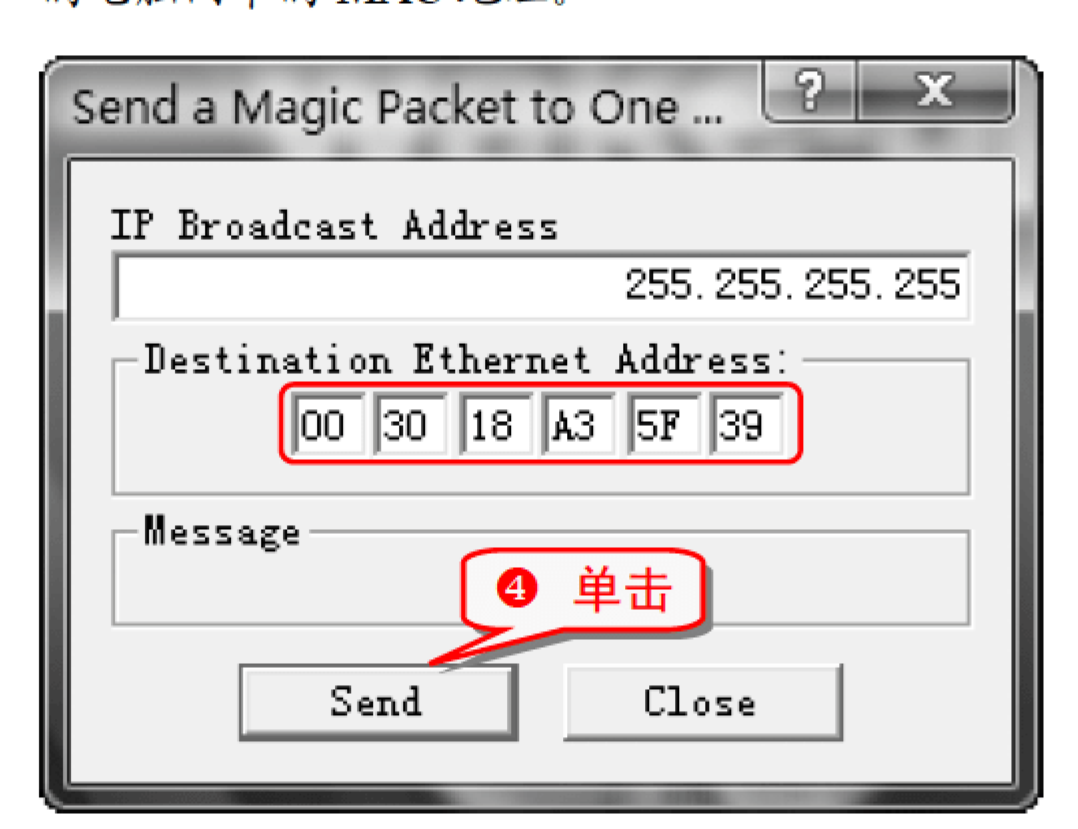
远程唤醒技术(Wake-on-LAN)是通过局域网实现远程开机的一种技术，能够随时启动局域网内的电脑。远程唤醒技术需要借助相应的网络管理软件才能实现。

目前，用于发送远程唤醒数据包的软件有 Magic Packet，多数网卡都能与之很好地兼容。

❶ 运行 Magpac.exe 程序，进入 Magic Packet 主界面。



❸ 在 Destination Ethernet Address: 选项组中输入欲唤醒的电脑网卡的 MAC 地址。



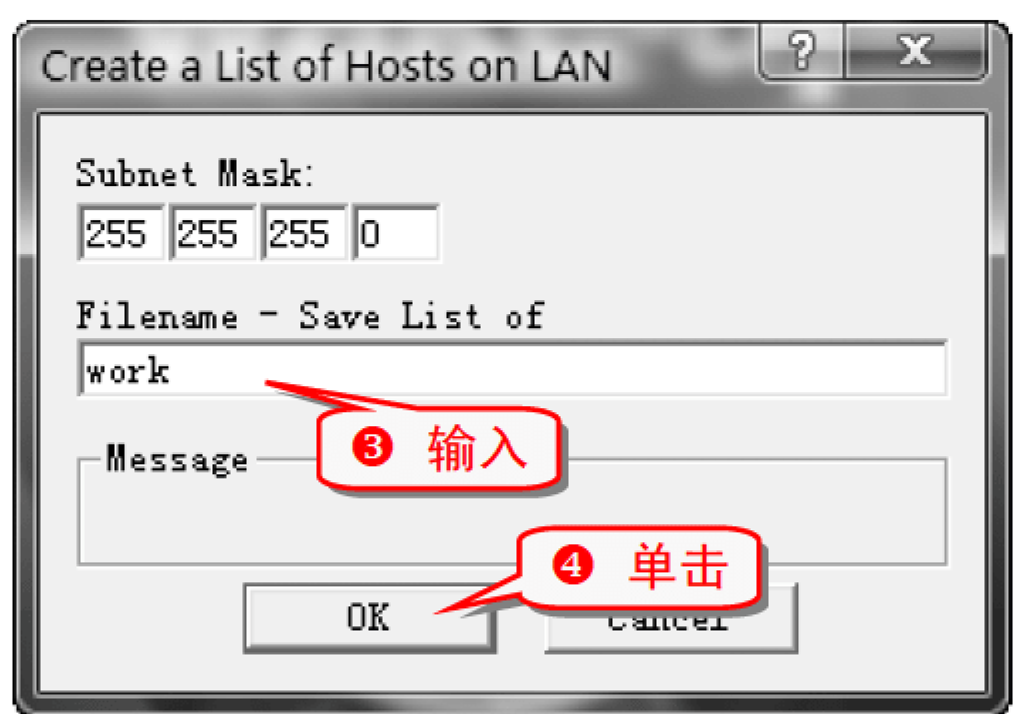
技巧229 使用 Magic Packet 远程唤醒多台电脑

使用 Magic Packet 不仅可以远程唤醒一台电脑，还可以远程唤醒多台电脑。

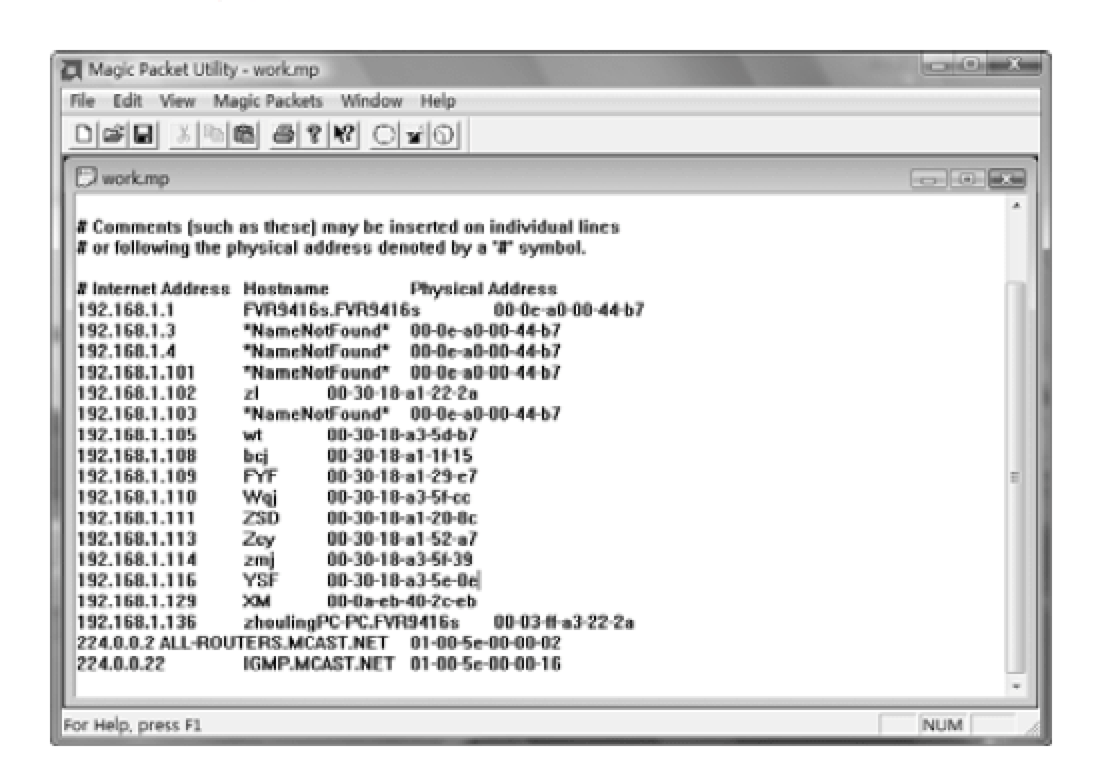
❶ 运行 Magpac.exe 程序，进入 Magic Packet 主界面。

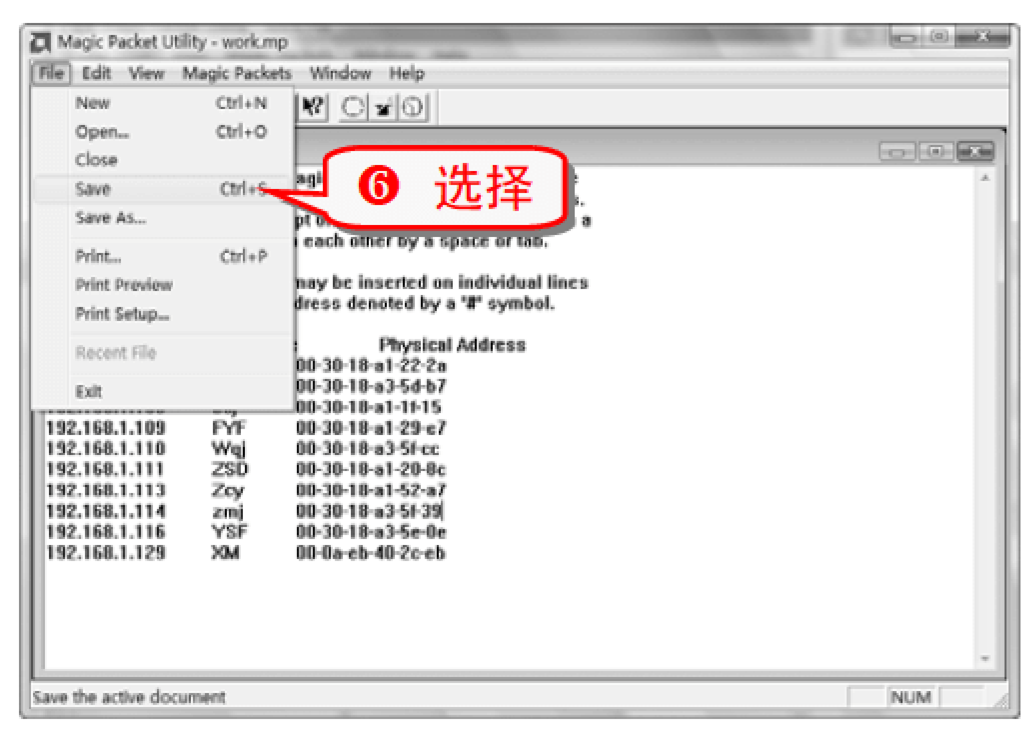


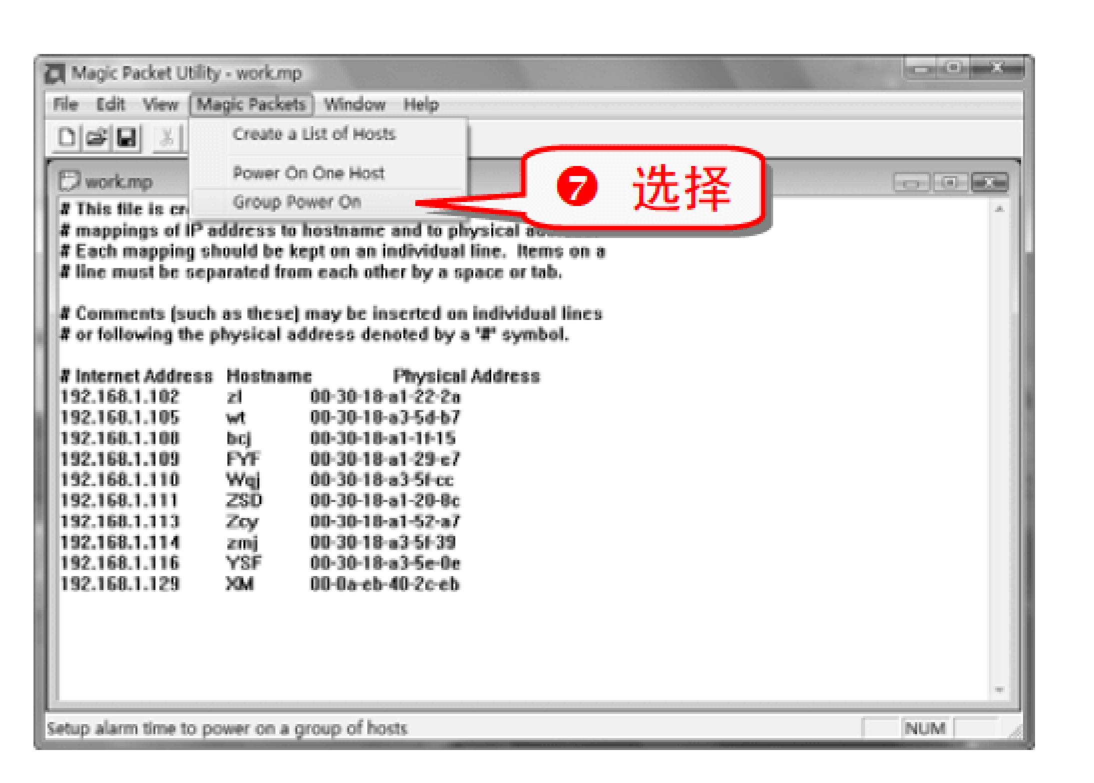


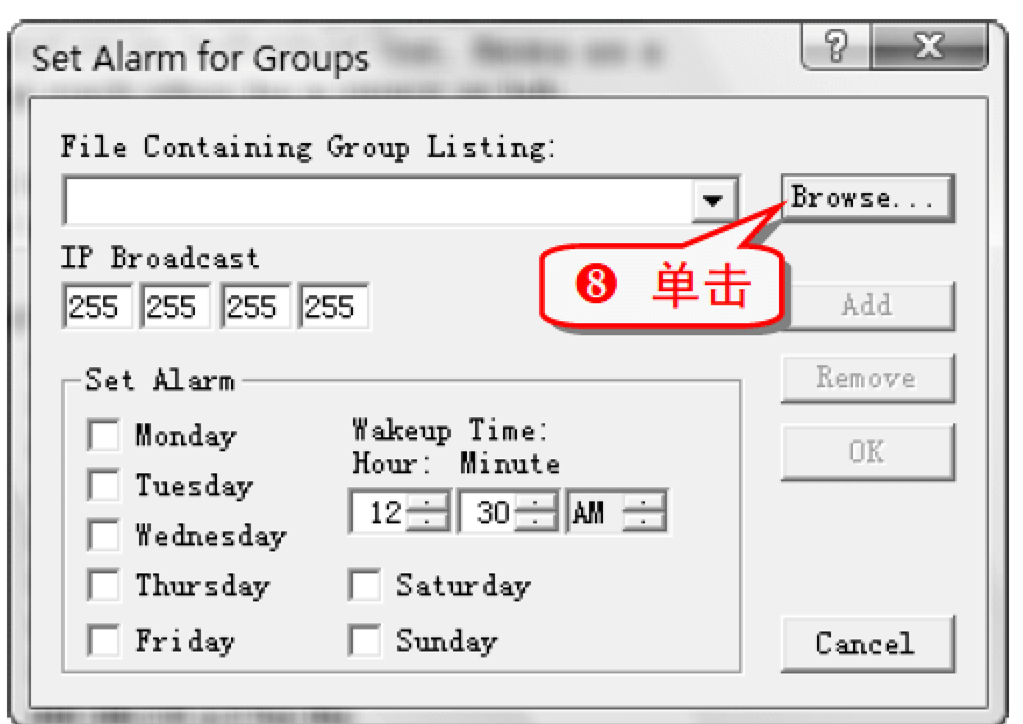


❺ 利用 Edit 菜单中 cut 命令，从列表中删除不需要进行远程唤醒的电脑。



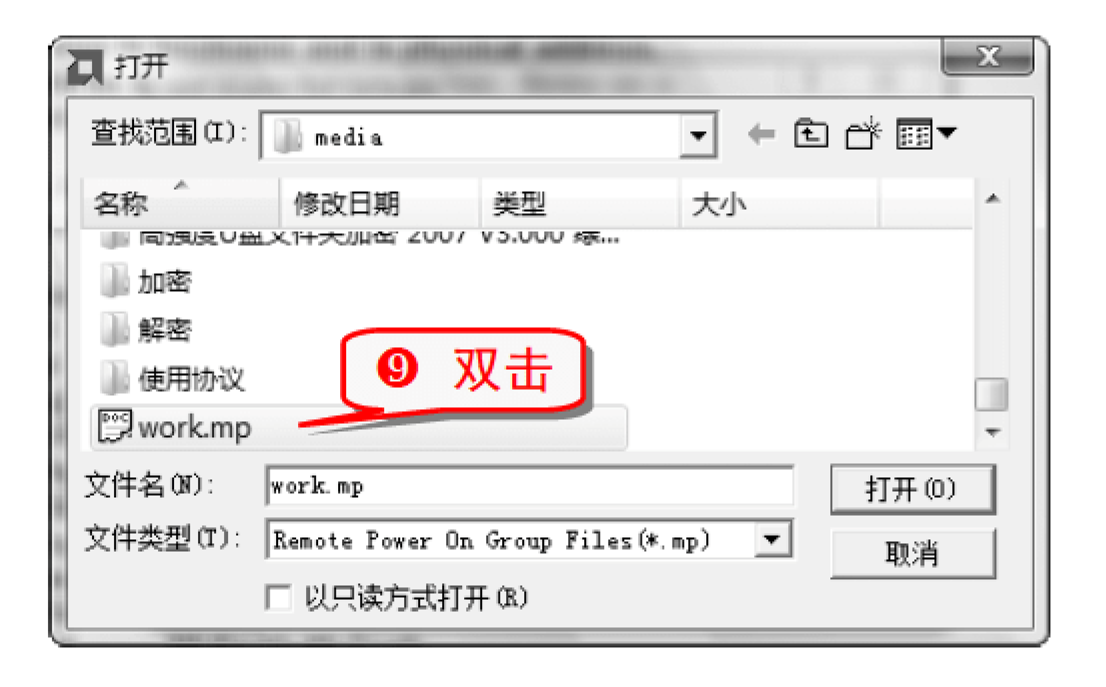






知　识　补　充

若要实现局域网内一组电脑的自动定时唤醒，可选中 Set Alarm for Groups 对话框中相应日期前的复选框并设置具体的唤醒时间。



❿ 返回 Set Alarm for Groups 对话框，依次单击 Add 和 OK 按钮，即可实现局域网内一组电脑的远程启动。

注　意　事　项

Magic Packe 可以从 ftp://ftp.amd.com/pub/npd/software/pcnet_family/drivers/magic_pkt.exe 下载。

技巧230　巧用流光

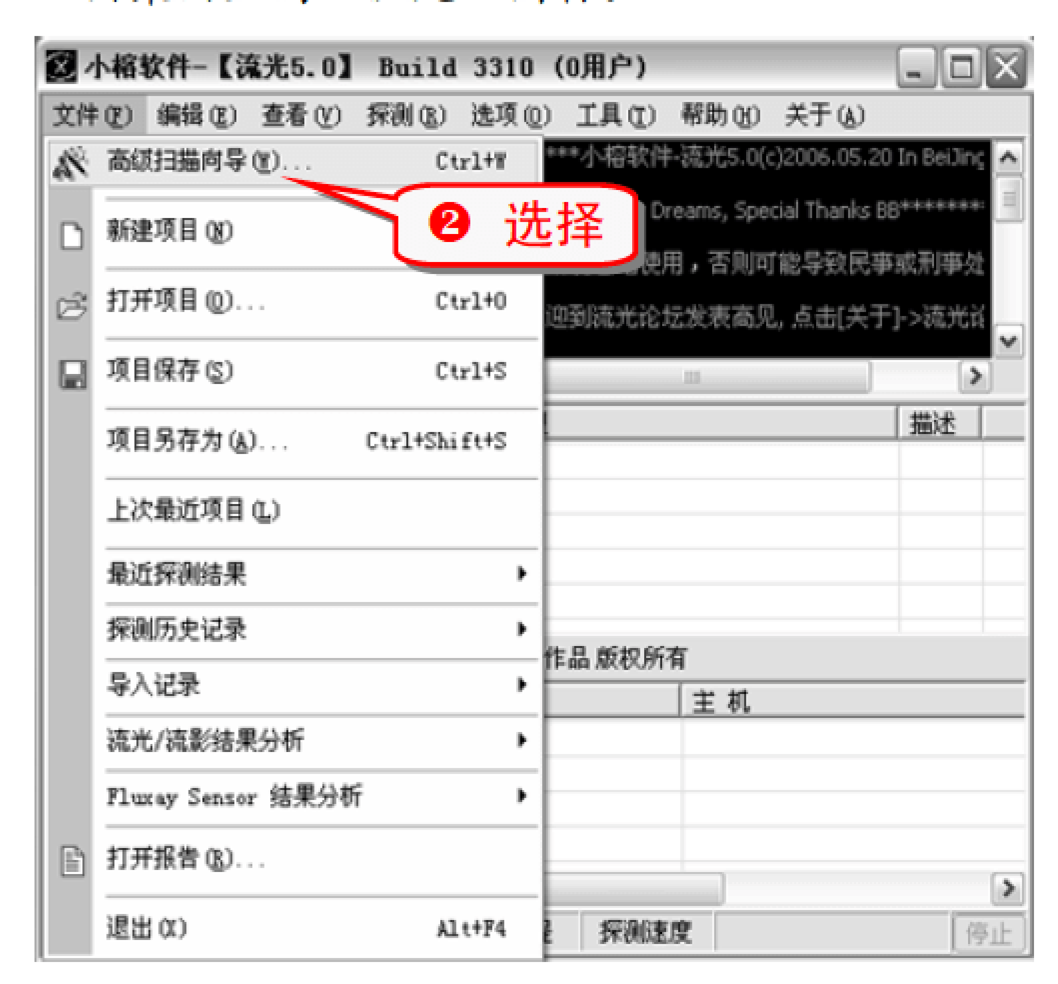
流光是一款强大的 FTP、POP3 解密工具，主要有以下功能。

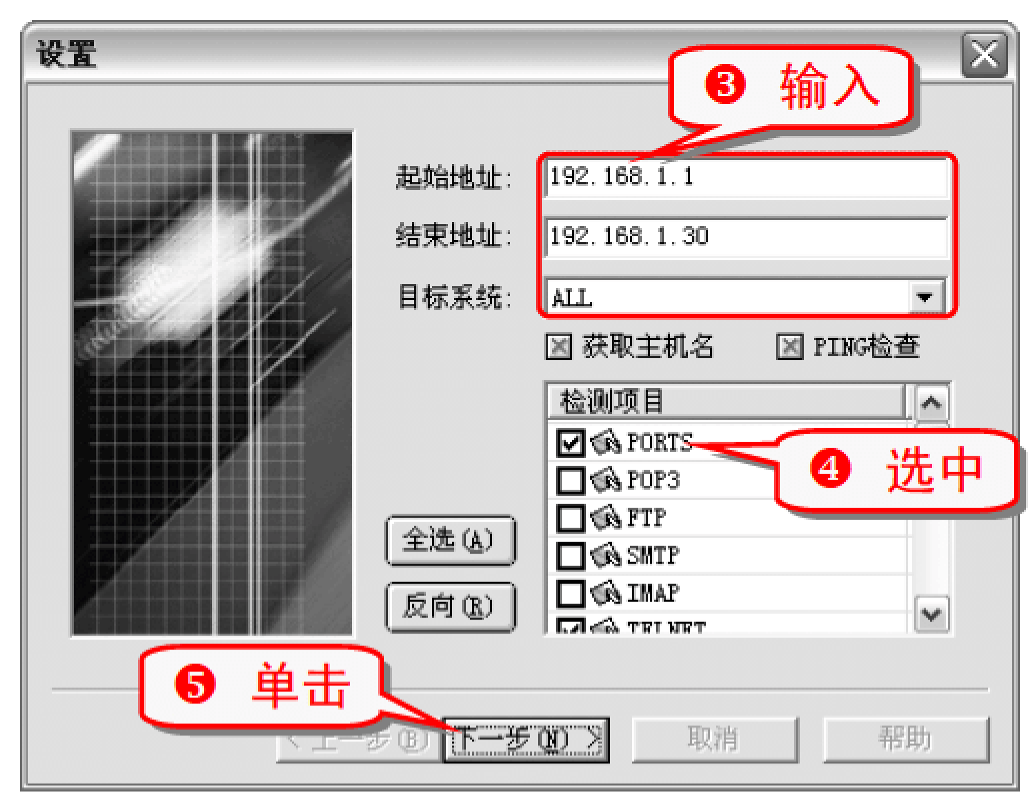
- 用于检测 POP3/FTP 主机中用户密码的安全漏洞。
- 多线程检测，消除系统中密码漏洞。
- 高效的用户流模式。
- 高效的服务器流模式，可同时对多台 POP3/FTP 主机进行检测。
- 最多 500 个线程探测。
- 线程超时设置，阻塞线程具有自杀功能，不会影响其他线程。
- 支持 10 个字典同时检测。
- 检测设置可作为项目保存。
- 取消了国内 IP 限制而且免费。

下面介绍使用流光进行扫描的操作步骤。

(1) 设置扫描项目

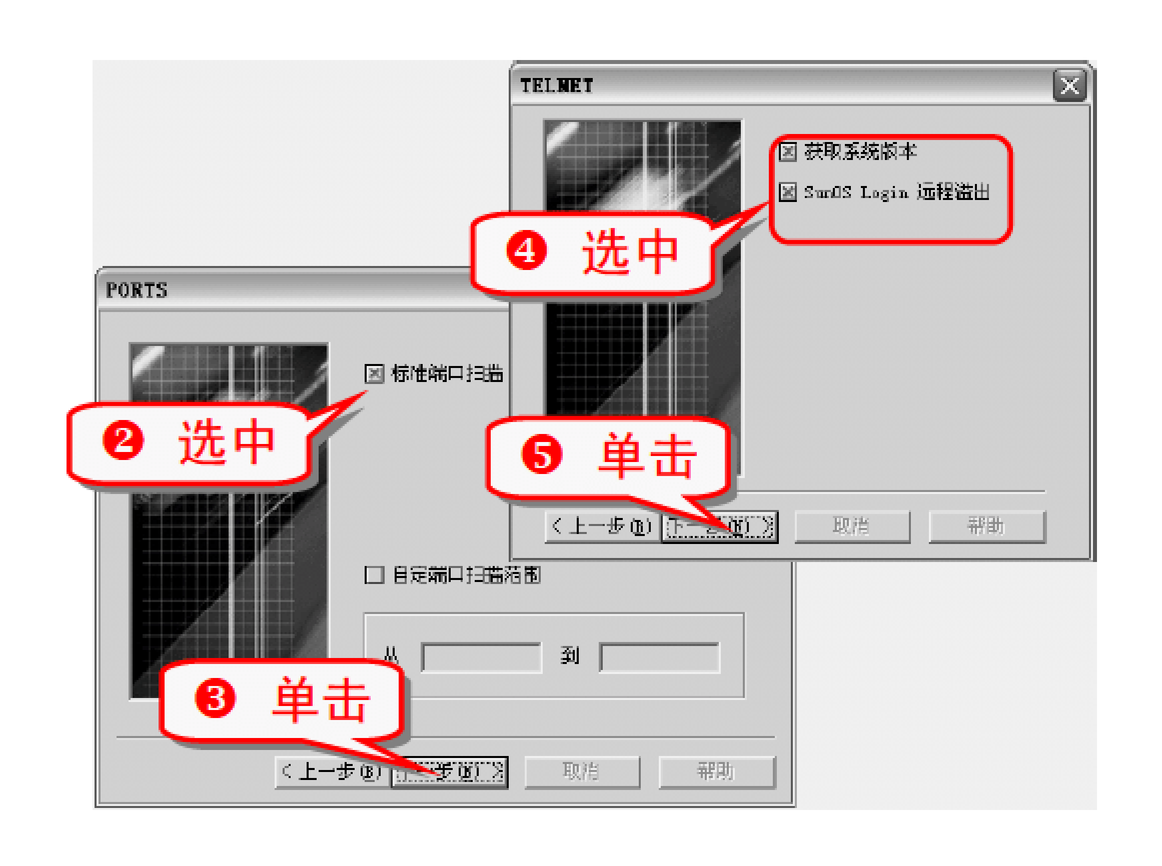
❶ 双击桌面上的“流光”图标。





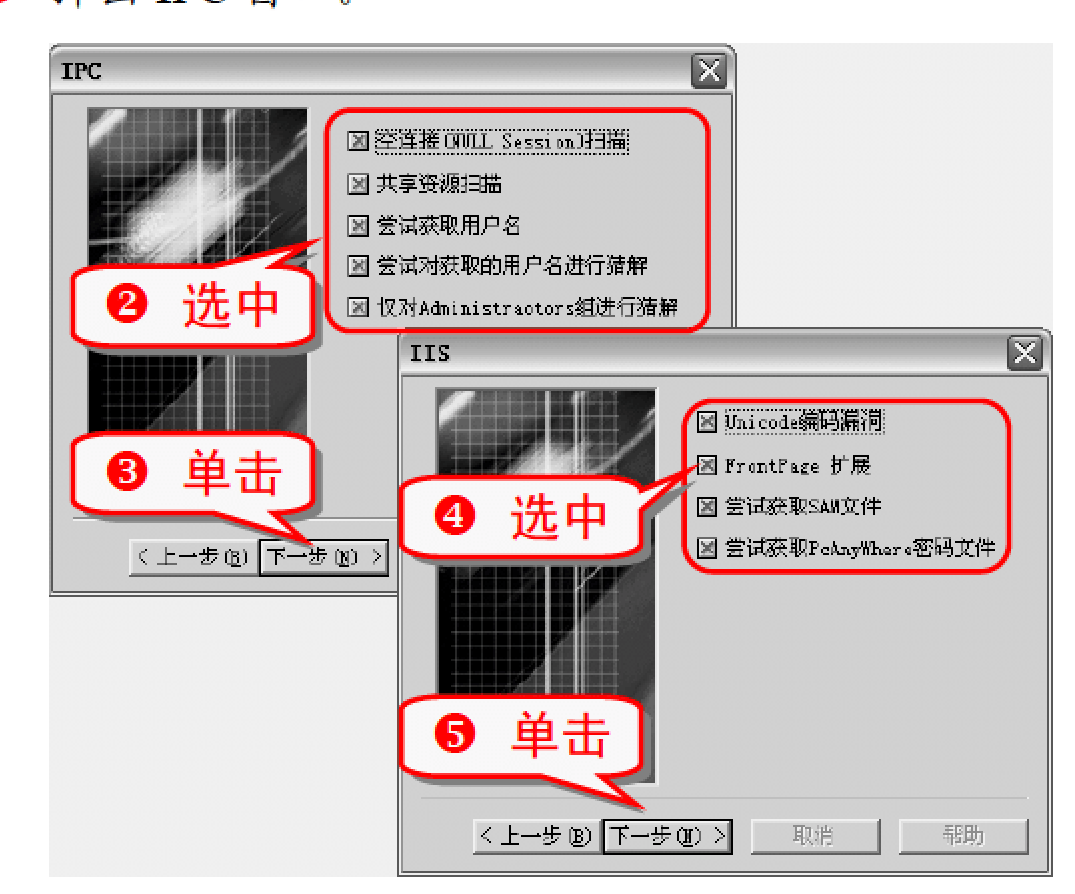
(2) 设置 PORTS 和 TELNET

❶ 设置好扫描项目后，弹出 PORTS 窗口。



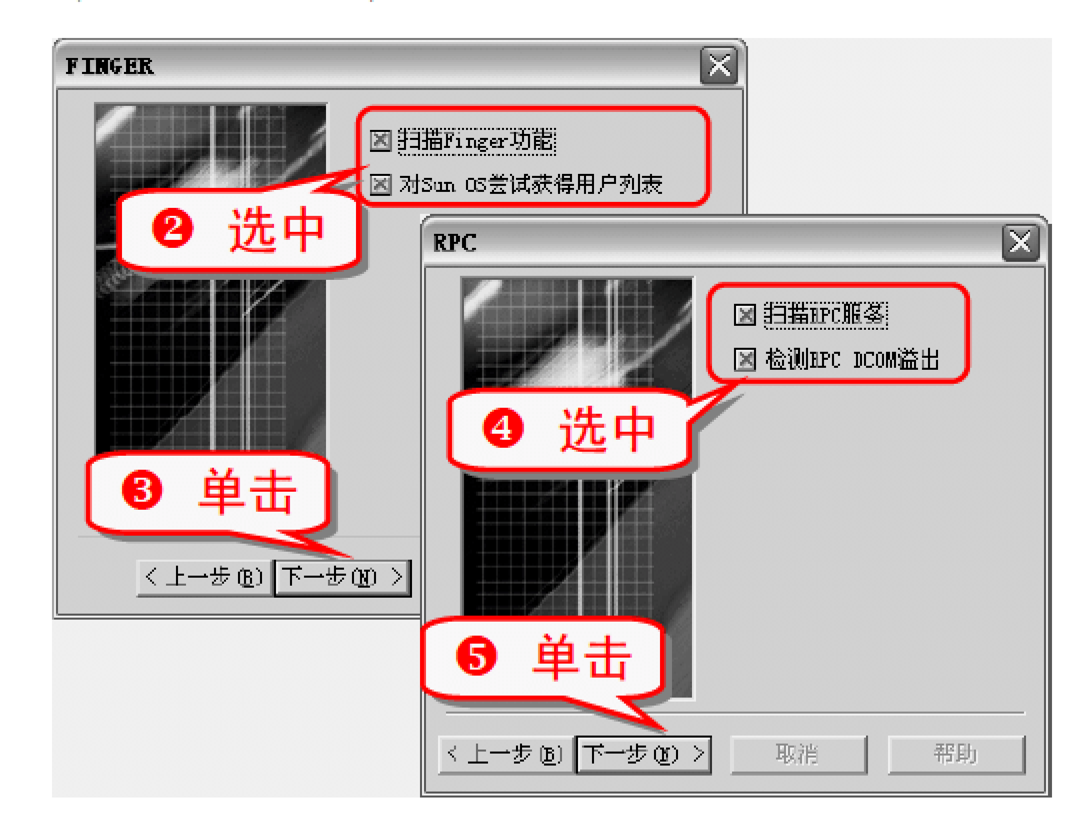
(3) 设置 IPC 和 IIS

❶ 弹出 IPC 窗口。



(4) 设置 FINGER 和 RPC

❶ 弹出 FINGER 窗口。



(5) 设置字典、报告保存和开发线程数目

❶ 弹出“选项”窗口。

❷ 在“猜解用户名字典”文本框中输入用户名字典文件的路径。



❸ 在“猜解密码字典”文本框中输入密码字典文件的路径。

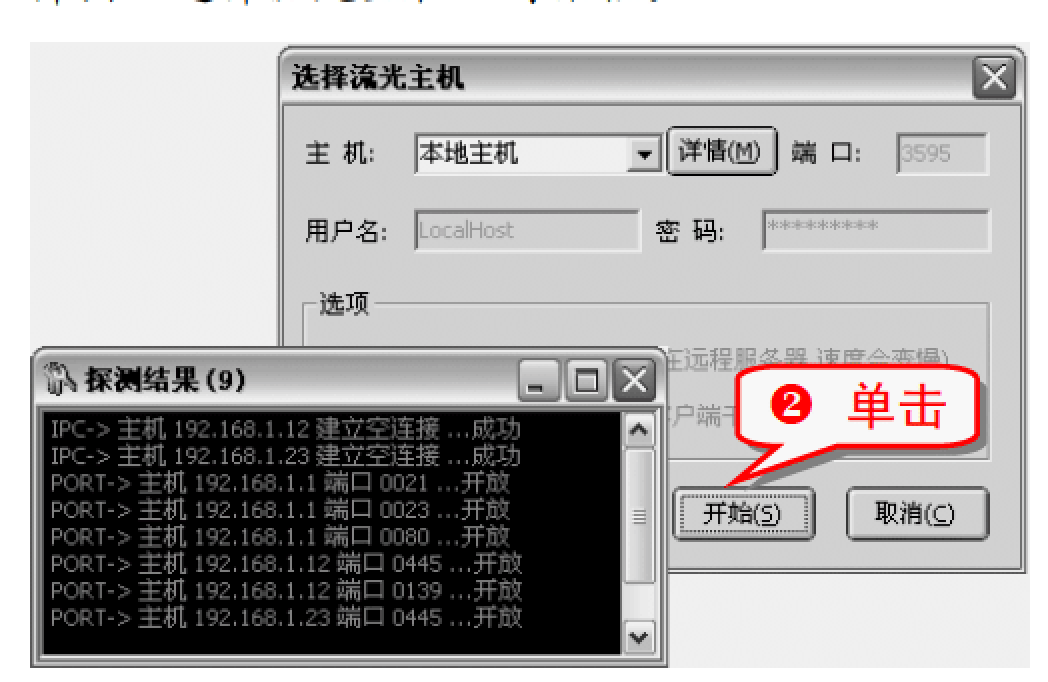
❹ 在“保存扫描报告”文本框中输入密码保存扫描报告的路径。

❺ 在“并发线程数目”数值框中输入进程数量。



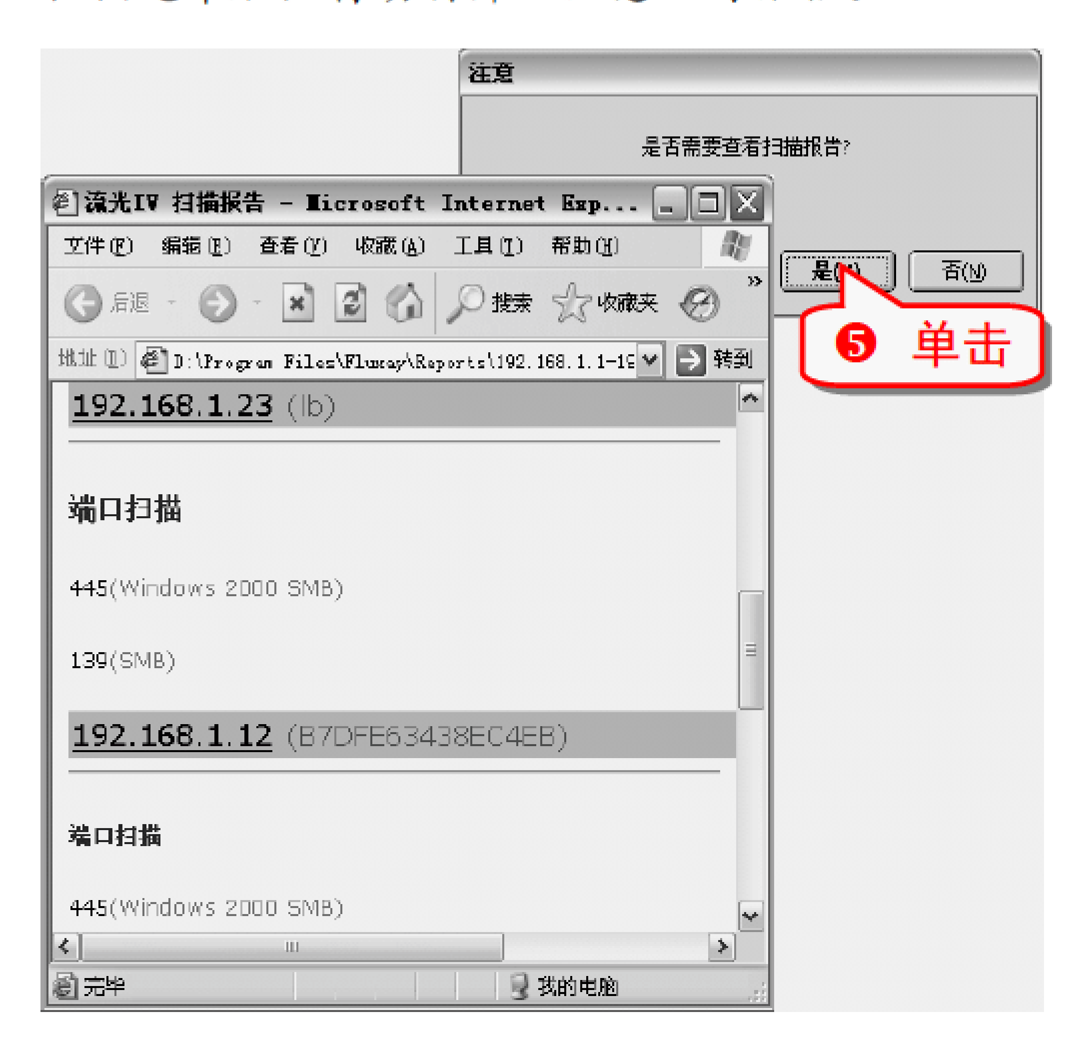
(6) 进行扫描

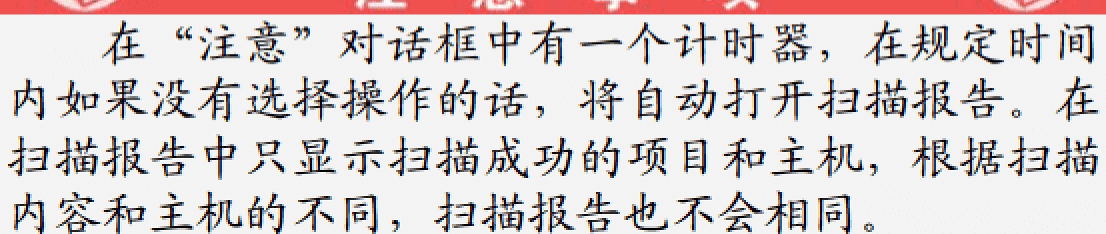
❶ 弹出“选择流光主机”对话框。



❸ 程序自动打开“探测结果”窗口，扫描后的即时结果显示在该窗口中。

❹ 扫描完毕后，自动打开“注意”对话框。





在“注意”对话框中有一个计时器，在规定时间内如果没有选择操作的话，将自动打开扫描报告。在扫描报告中只显示扫描成功的项目和主机，根据扫描内容和主机的不同，扫描报告也不会相同。

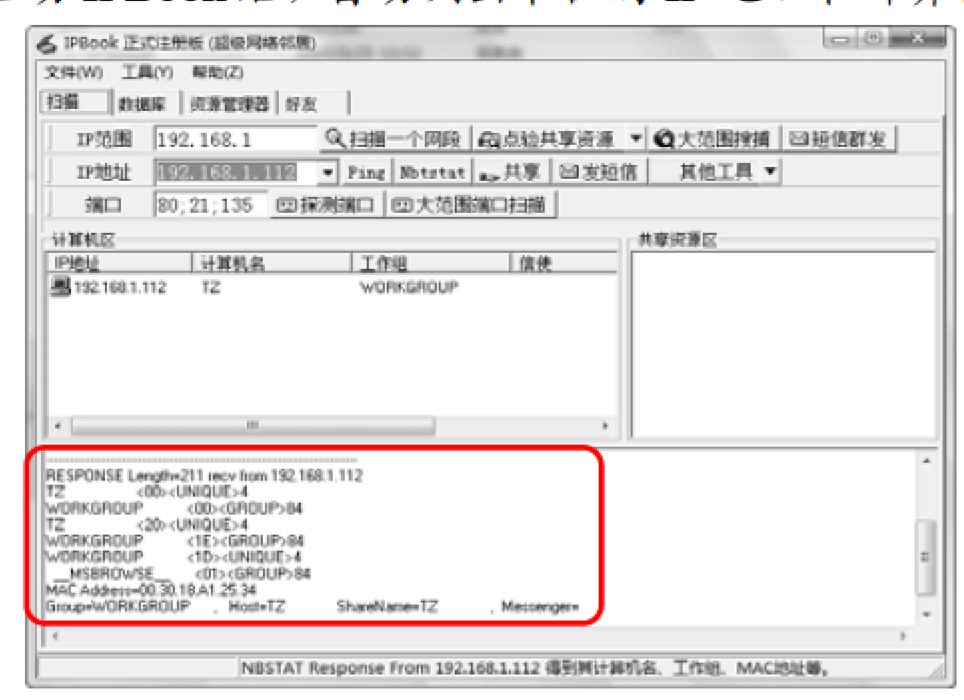
技巧231　巧用超级网络邻居

IPBook(超级网络邻居)是一款小巧的搜索共享资源及 FTP 共享的工具，软件解压后就能直接运行，无需安装。主要功能包括以下几种。

- 搜索 Internet 上任意网段机器的共享资源。并且可以打开共享资源，功能类似于 Windows 的网络邻居。
- 搜索 HTTP 服务，FTP 服务及隐藏共享。
- 给指定的计算机发送弹出式短消息。
- 查出自己的 IP 地址计算机名和 MAC 地址等等。
- 查出任意 IP 地址的计算机名，工作组，MAC 地址等等。
- 可以自动将查出的主要信息存储起来，以便下次查看。并且可以将其输出到文本文件中。
- 对指定的 IP 地址进行 Ping、Nbtstat，检测端口是否开放。

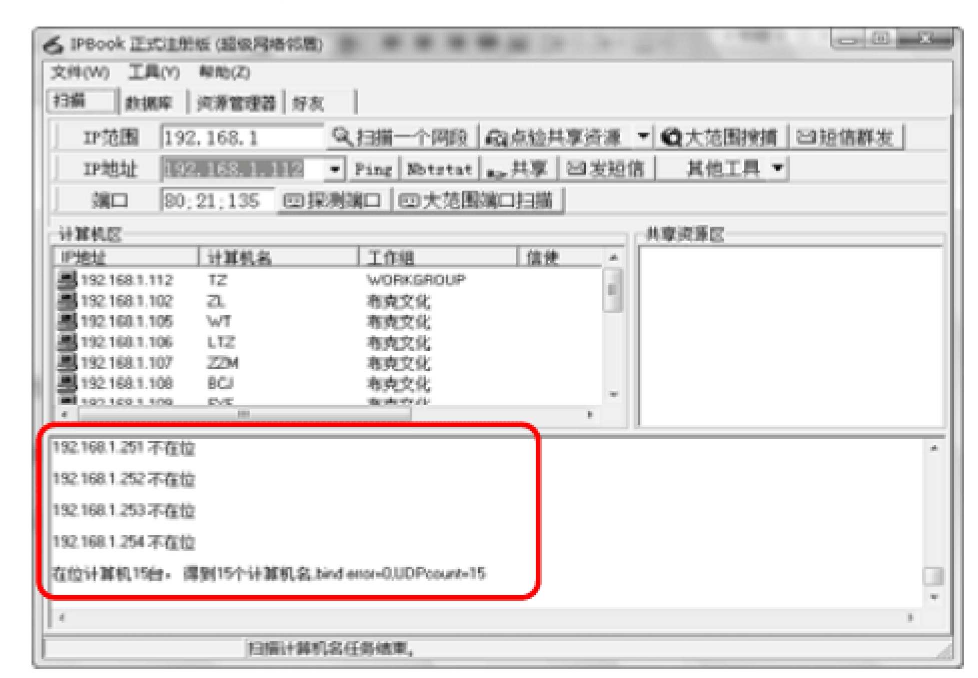
(1) 检测本地 IP 地址和计算机名

启动 IPBook 后，自动测出本机的 IP 地址和计算机名。

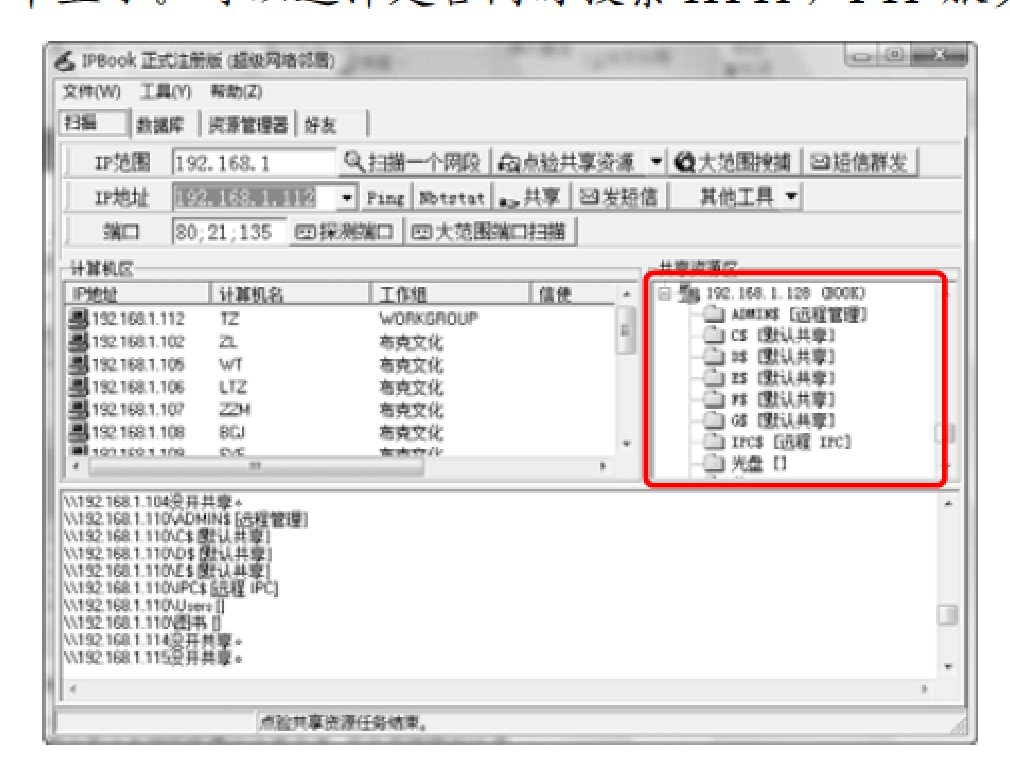


(2) 查看本网段所有计算机的计算机名与共享资源

❶ 单击“扫描一个网段”按钮，在计算机区的列表框中显示的就是本网段所有开启计算机的详细情况。其中有 IP 地址，计算机名，工作组以及信使名等等。

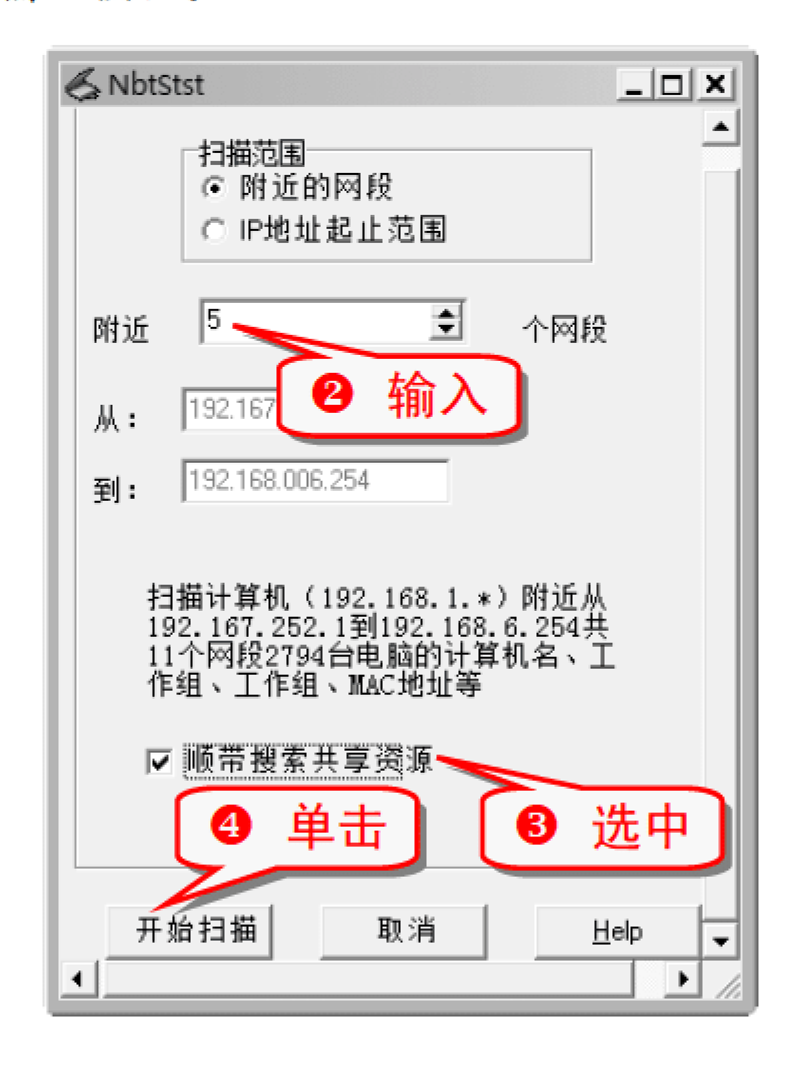


❷ 所有计算机情况查完后，单击“点验共享资源”按钮，本网段计算机的共享资源在共享资源区的树状列表框中显示。可以选择是否同时搜索 HTTP，FTP 服务。



(3) 检查任意网段的所有计算机的计算机名与共享资源

❶ 将本网段 IP 地址范围改成想要查的地址范围，以**.**.**的形式显示的就是网段范围。然后单击“大范围搜捕”按钮。



技巧232 用 S 扫描器扫描开放端口

S 扫描器是针对微软 ms04045 漏洞开发的一个程序，现在已经变成黑客手中的武器了，经常被用来扫描开放端口。它有如下功能。

- 两种不同的扫描方式(SYN 扫描和 connect 扫描)。
- 可以扫描单个 IP 或 IP 段所有端口。
- 可以扫描单个 IP 或 IP 段单个端口。
- 可以扫描单个 IP 或 IP 段用户定义的端口。
- 可以显示打开端口的 banner。
- 可将结果写入文件。
- TCP 扫描可自定义线程数。

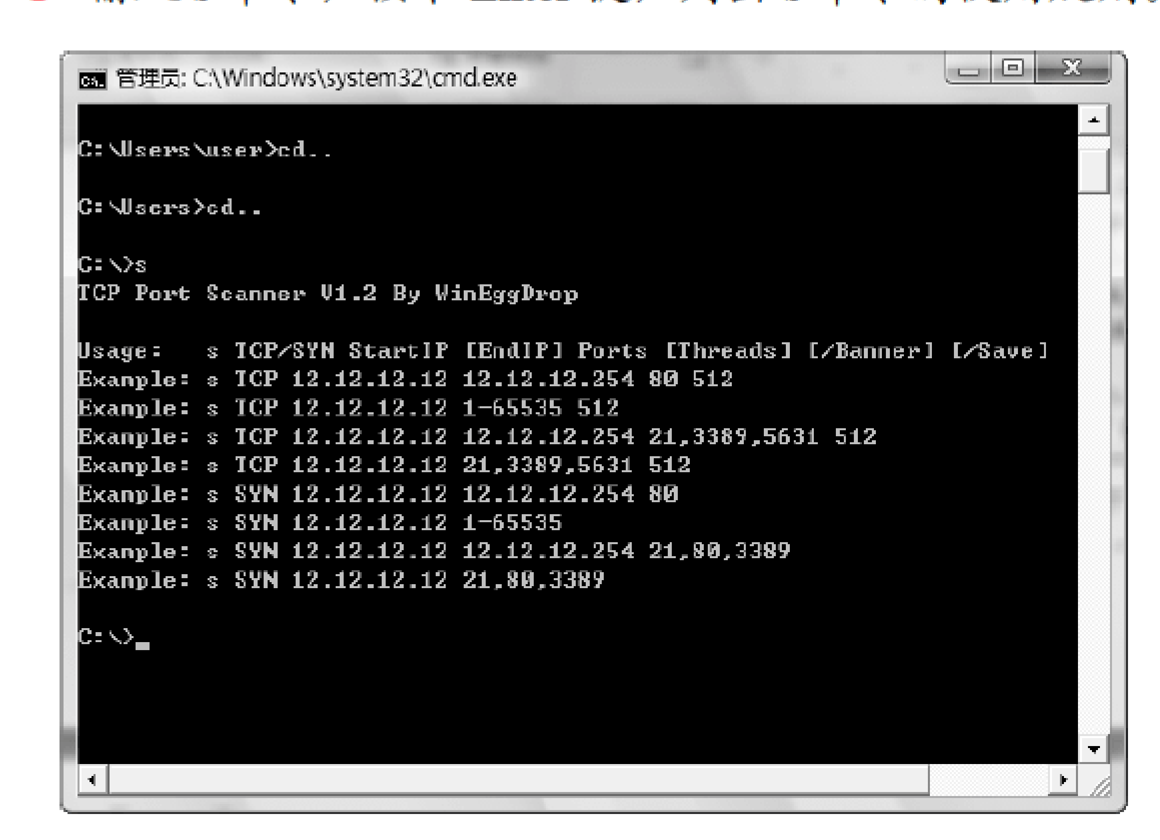
❶ 将下载的 S 扫描器的可执行文件放到 C 盘的根目录下。

❷ 打开“运行”对话框，输入 cmd 命令，按下 Enter 键，打开“命令提示符”窗口。

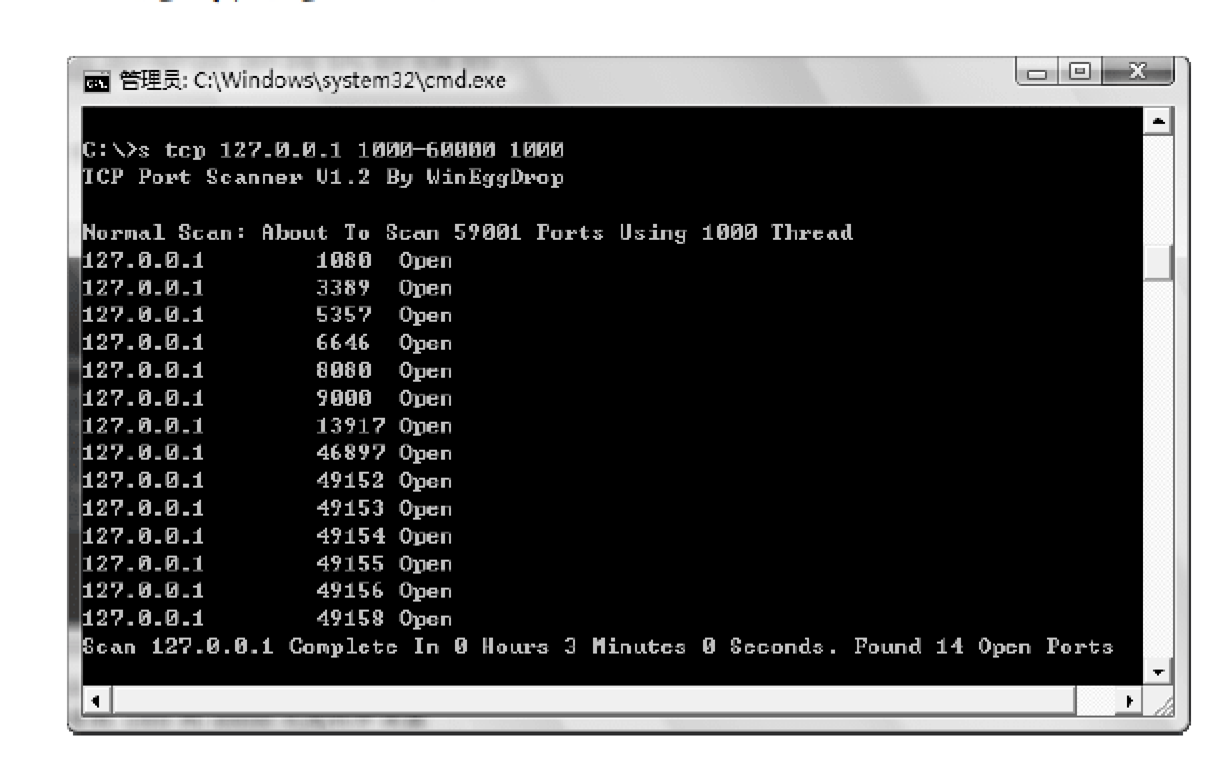
❸ 输入 cd..命令，按下 Enter 键。

❹ 再输入 cd..命令，按下 Enter 键。

❺ 输入 s 命令，按下 Enter 键，列出 s 命令的使用规则。



❻ 输入 s TCP 127.0.0.1 1000-60000 1000 命令，按下 Enter 键，扫描本机 1000 到 60000 之间的开放端口，最大并发线程是 1000。



技巧233 巧用 SuperScan

SuperScan 是一款优秀的扫描软件，除了端口扫描的功能以外，还有很多其他的功能。

- 检验 IP 是否在线。
- IP 和域名相互转换。
- 检验目标电脑提供的服务类别。
- 检验一段范围内目标电脑是否在线以及端口情况。

软件中自带一个木马端口列表文件 trojans.lst，用于检验当前电脑是否存在木马，同时还可以自定义修改该列表。SuperScan 主界面如下图所示。

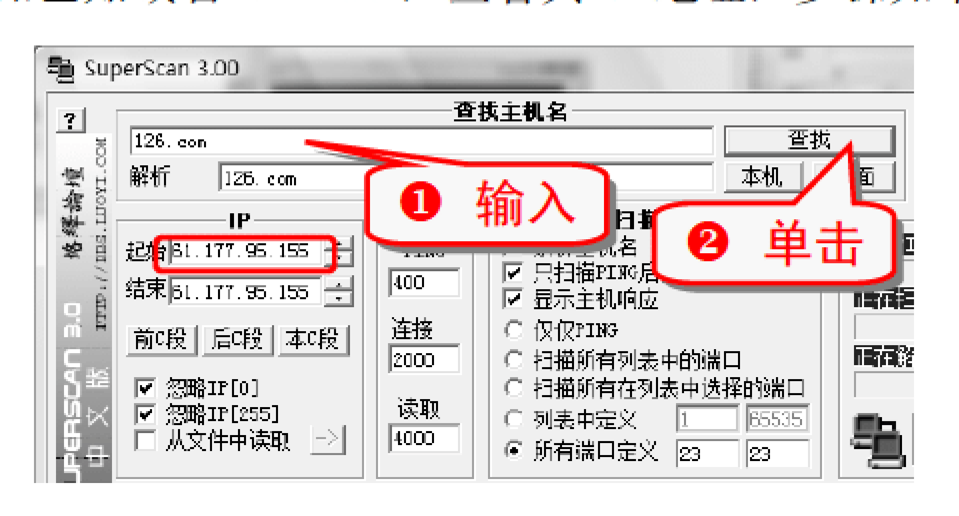




(1) 域名和 IP 相互转换

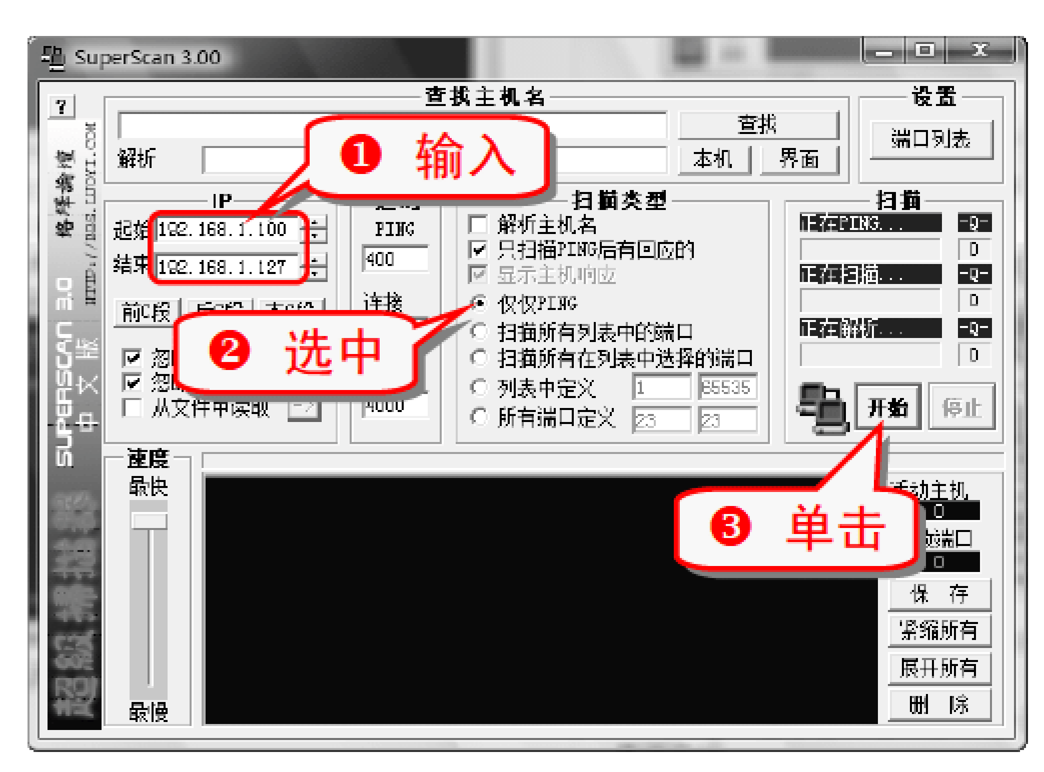
SuperScan 可以根据域名查得 IP 地址，或者根据 IP 地址查得域名。

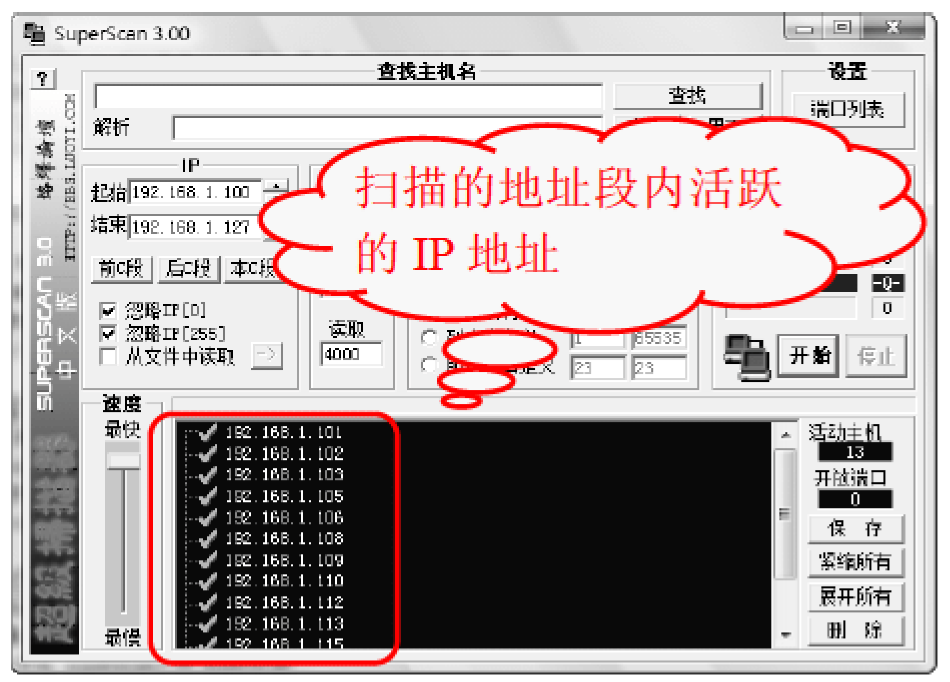
如已知域名 126.com，查看其 IP 地址，步骤如下。



(2) 使用 Ping 功能

Ping 的主要目的是检测目标 IP 是否活跃，即目标电脑是否在线。

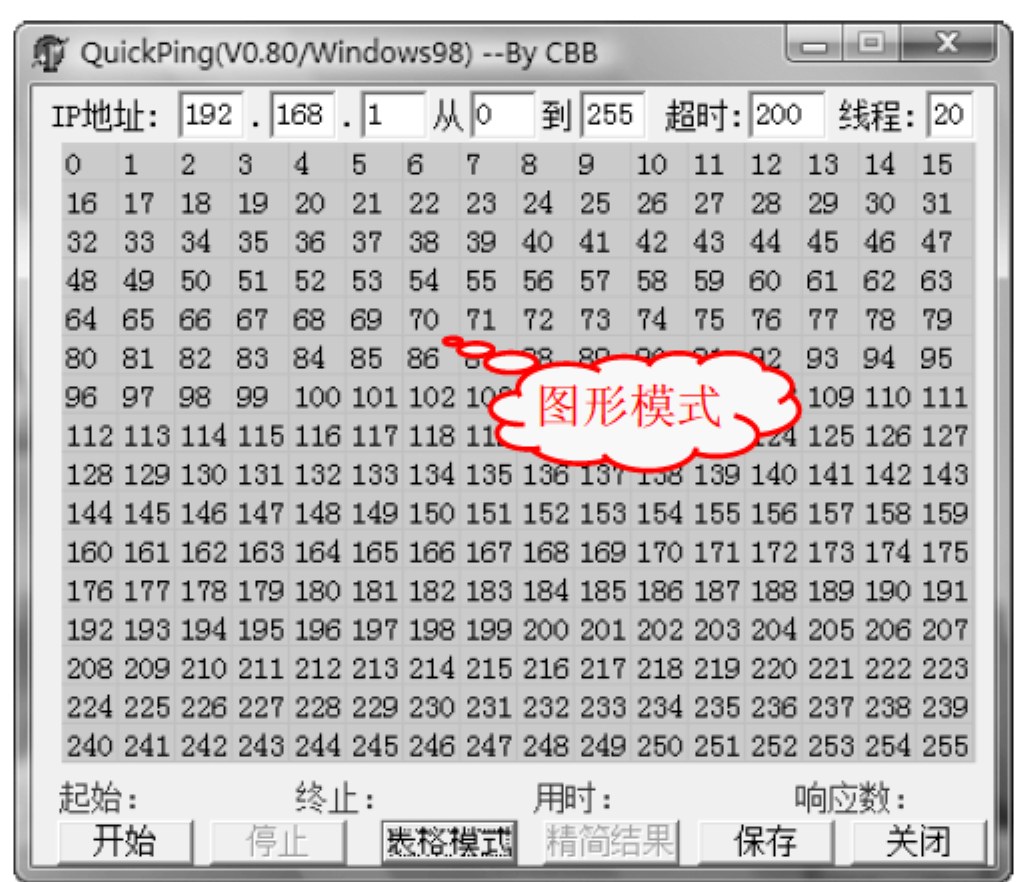


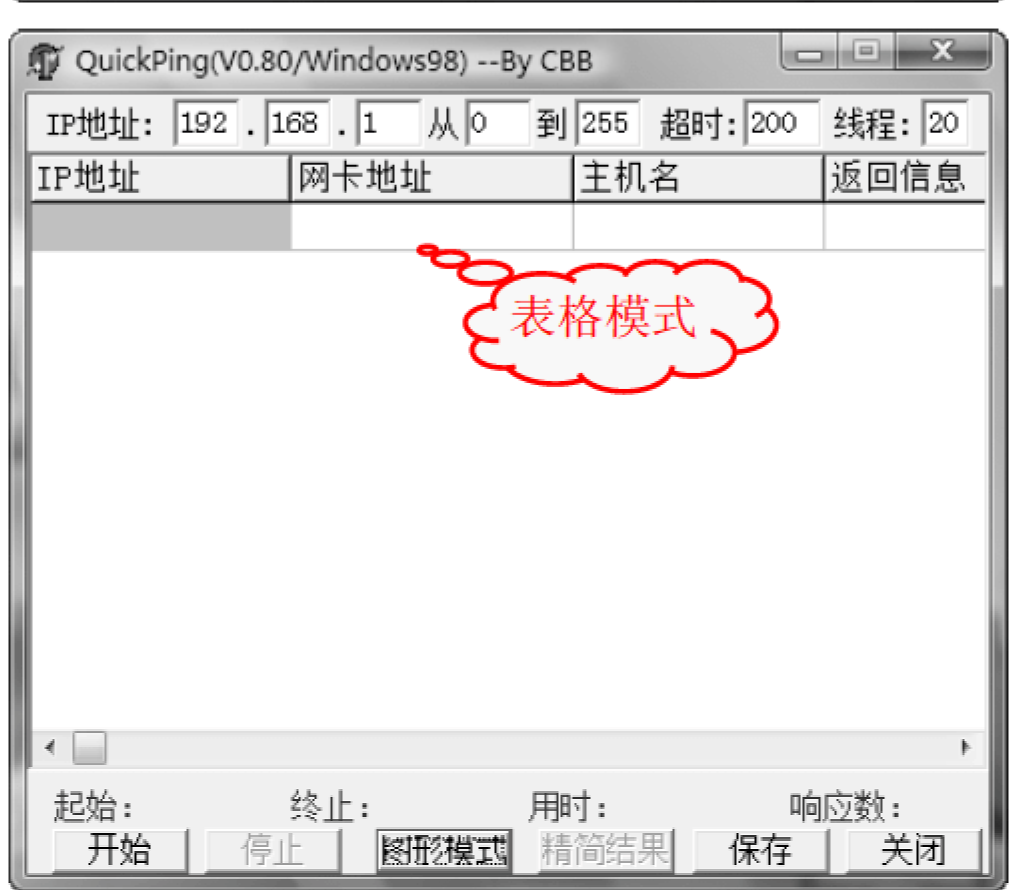


技巧234　快速 Ping 扫描工具

快速 Ping 扫描工具是一款快速 Ping 活跃主机的小工具，可以从网上下载。其扫描速度非常快，是黑客攻击的利器。

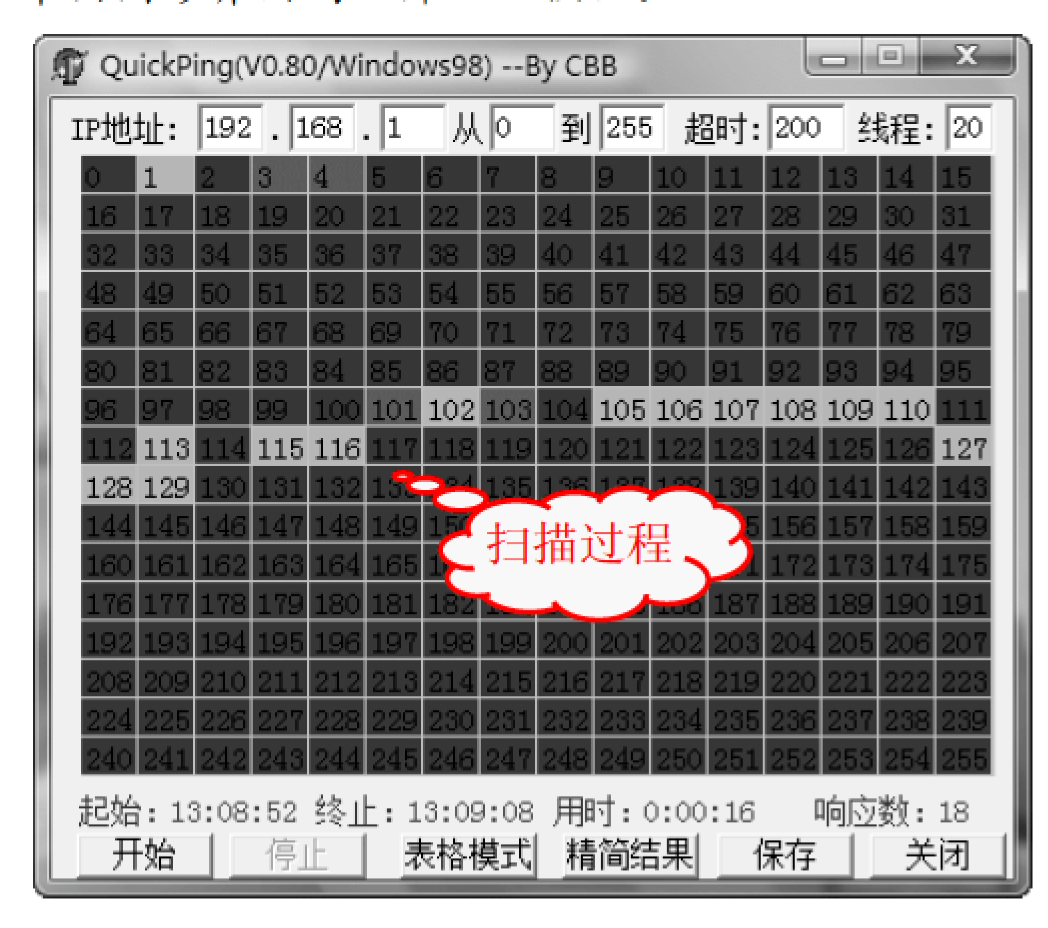
该工具有两个模式，分别是图形模式和表格模式。

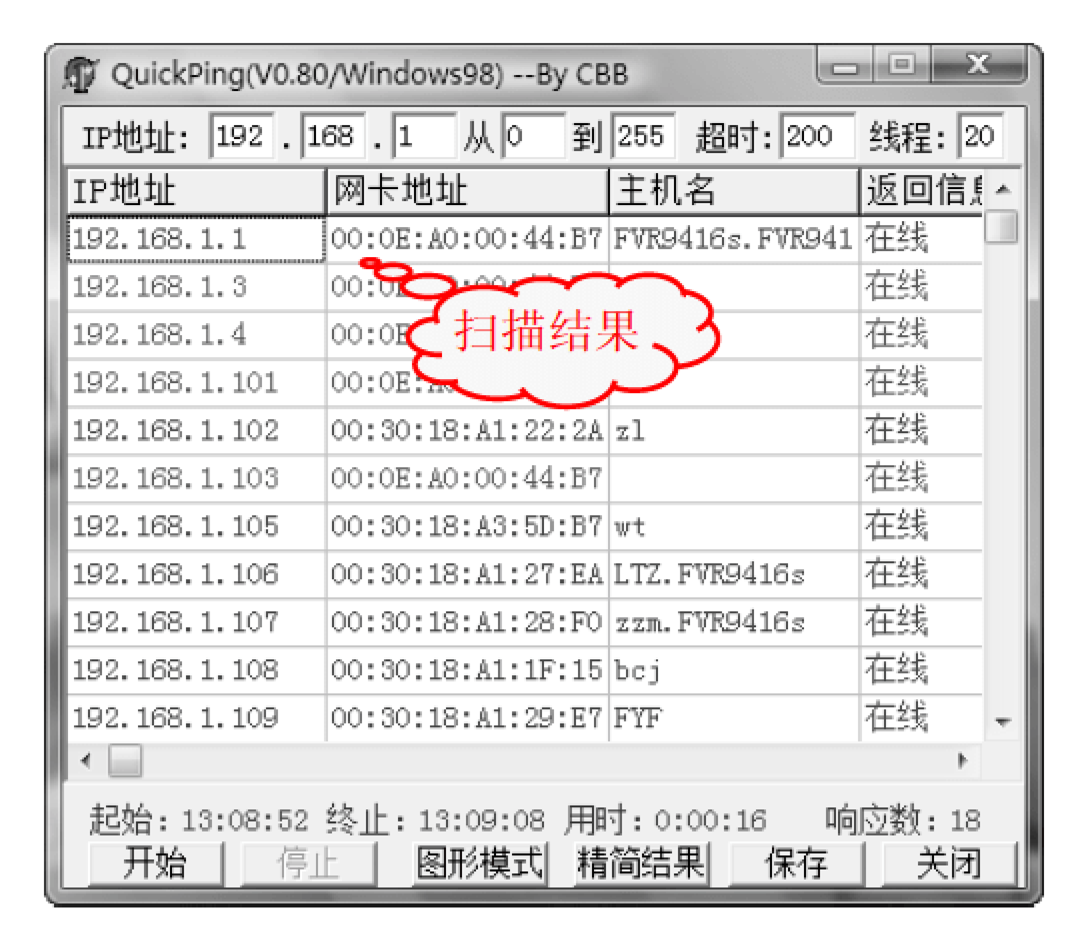




扫描过程如下。

单击图形界面的“开始”按钮。





技巧235 ScanPort 扫描工具

ScanPort 是一款小巧的网络端口扫描工具，是绿色软件。其扫描界面简单明了，操作方便。操作方法如下所示。

❶ 下载 ScanPort，双击即可运行。





专题九　彻底查杀病毒

内容导航

杀毒软件是电脑中不可缺少的应用软件，木马和病毒会破坏系统文件甚至是硬件，选择合适的杀毒软件，可以很好地防御病毒和木马的攻击，保护电脑的安全。

热点快报

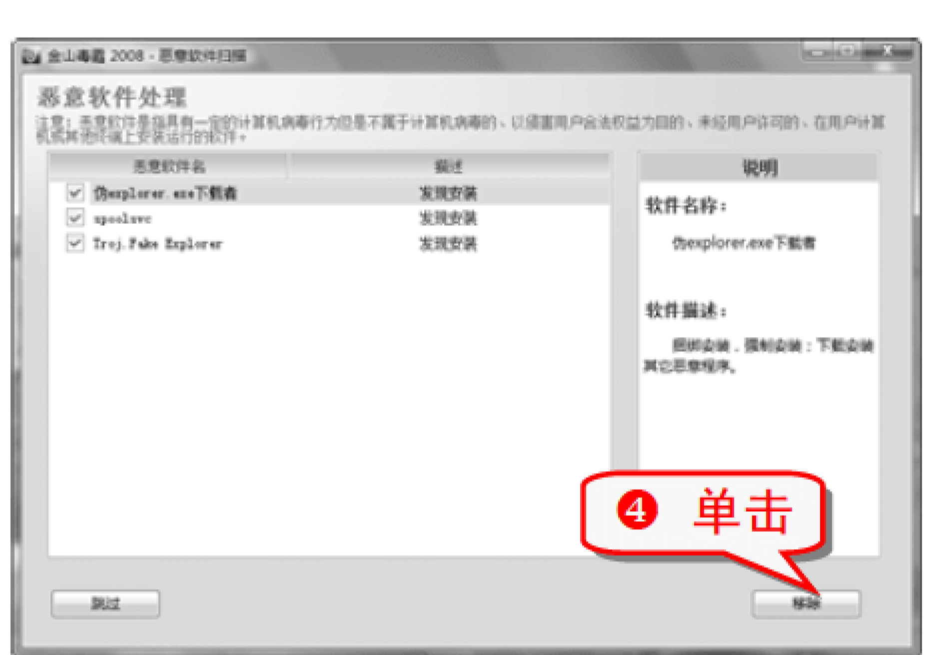
- 查杀病毒木马技巧
- 查杀恶意软件技巧
- 清理垃圾文件技巧
- 修复系统漏洞技巧
- 检查系统安全性
- 设置程序黑白名单

技巧236　使用金山毒霸查杀病毒木马

金山毒霸是金山公司推出的一款比较好的杀毒软件，能实现系统的快速杀毒。

❶ 双击“金山毒霸”图标，进入程序运行主界面。



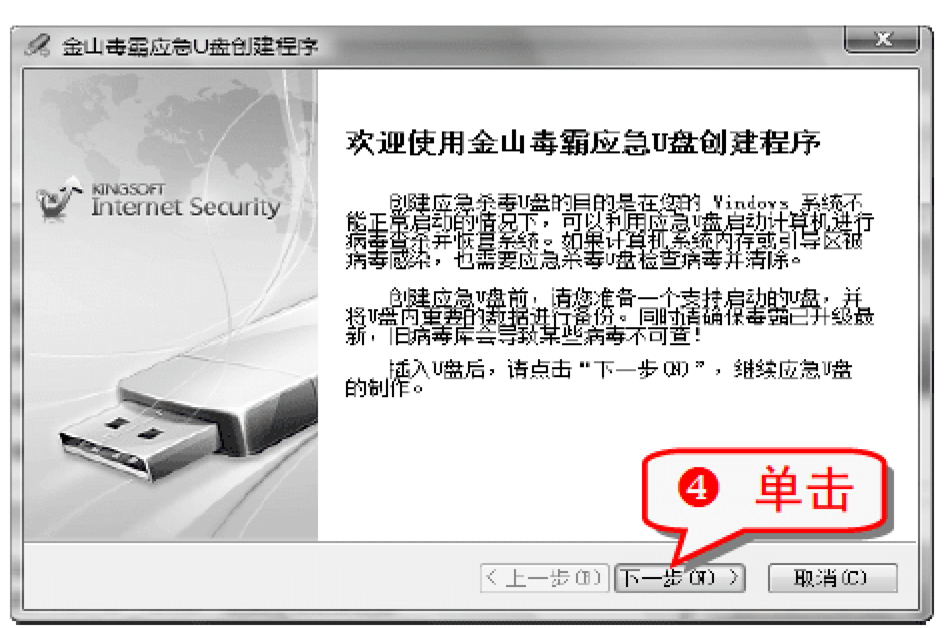


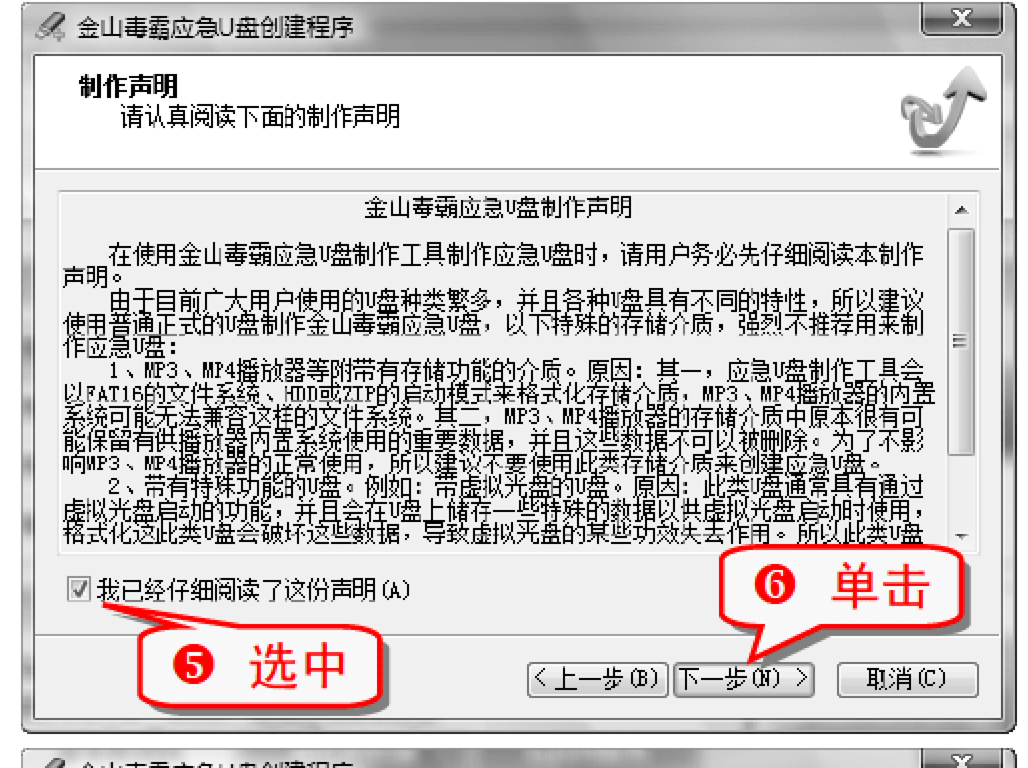
技巧237　使用金山毒霸创建应急 U 盘

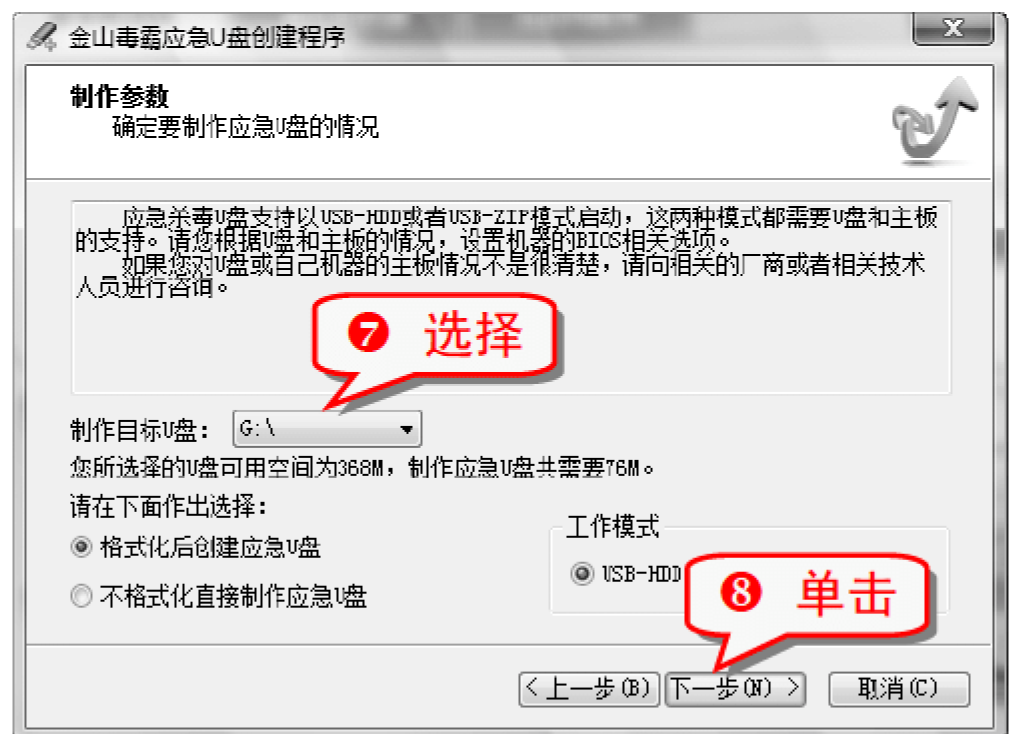
当系统不能正常启动时，可以使用金山毒霸创建的应急 U 盘启动系统。

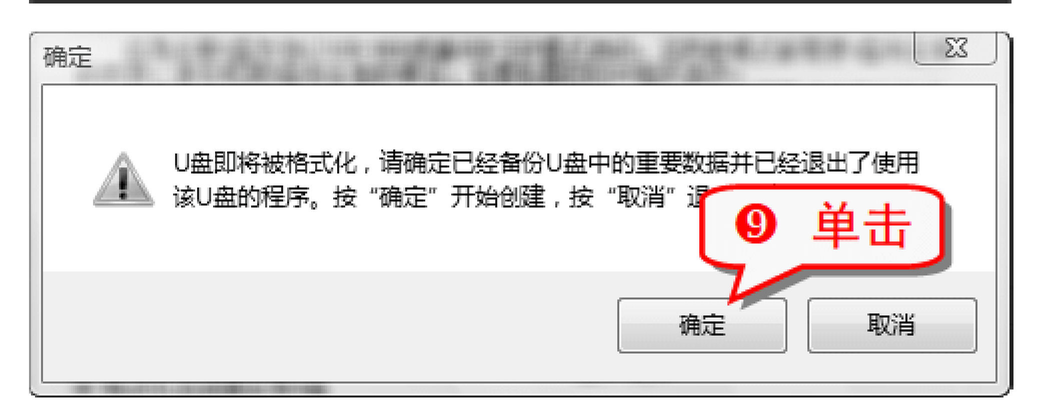
❶ 双击“金山毒霸”图标，进入程序运行主界面。

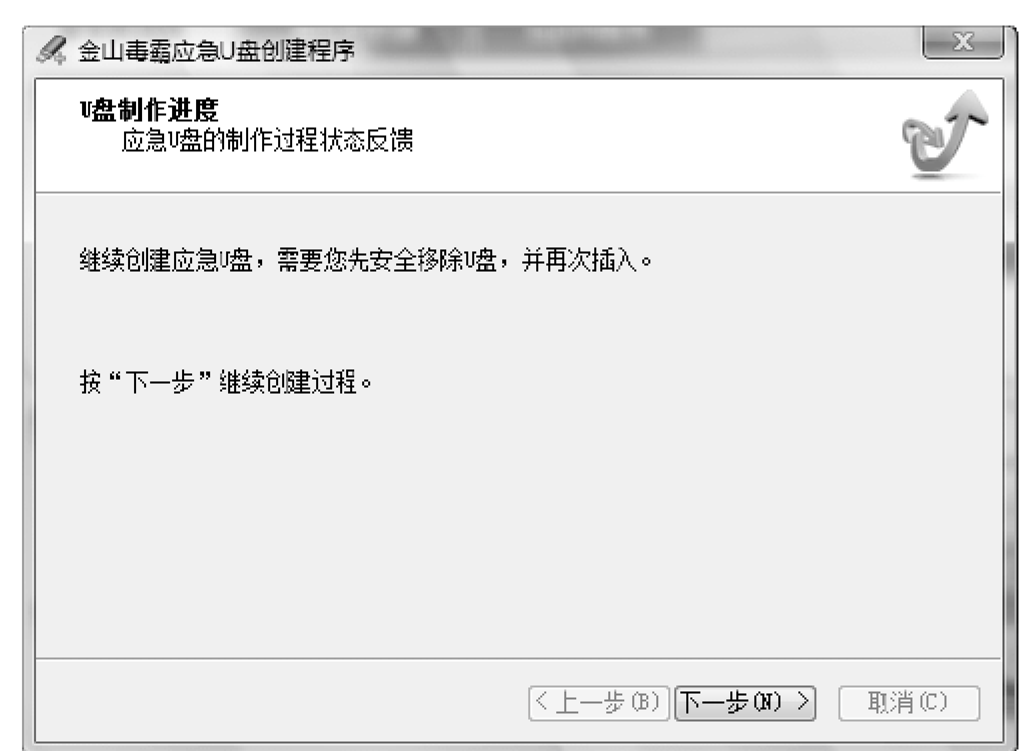










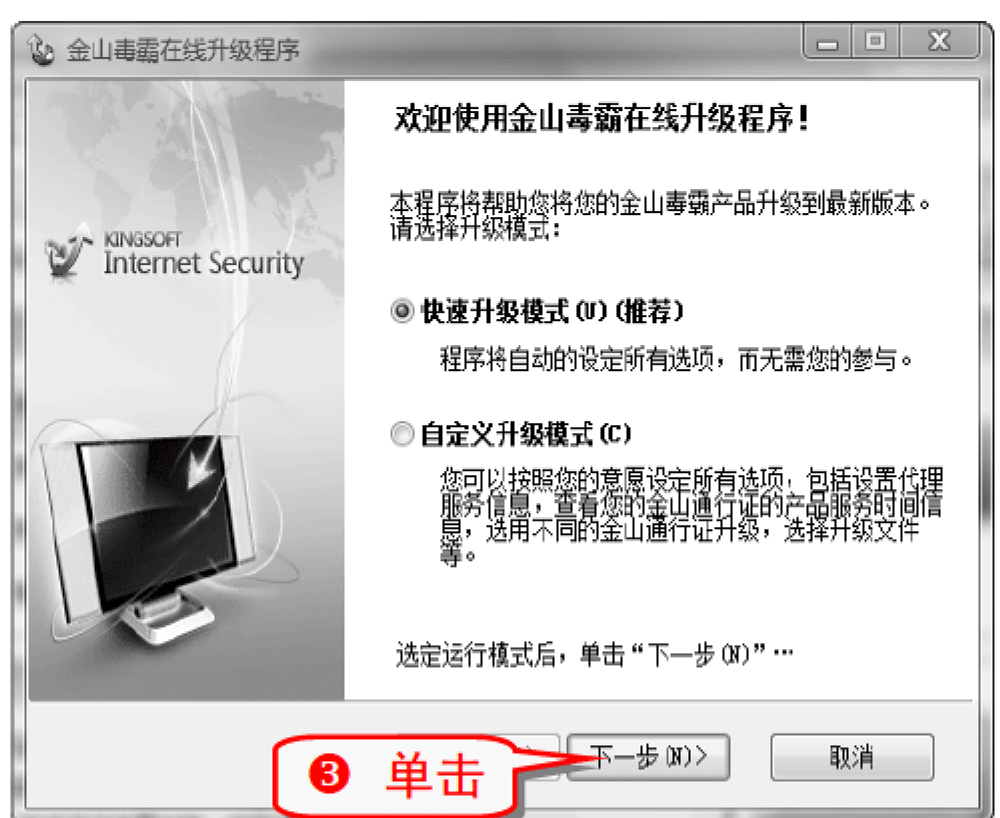


❿ 先移除U盘再将其插入，单击“下一步”按钮，再单击“完成”按钮。

技巧238　在线升级金山毒霸

升级分“快速升级”和“自定义升级”两种模式，用户可根据需要自由选择。





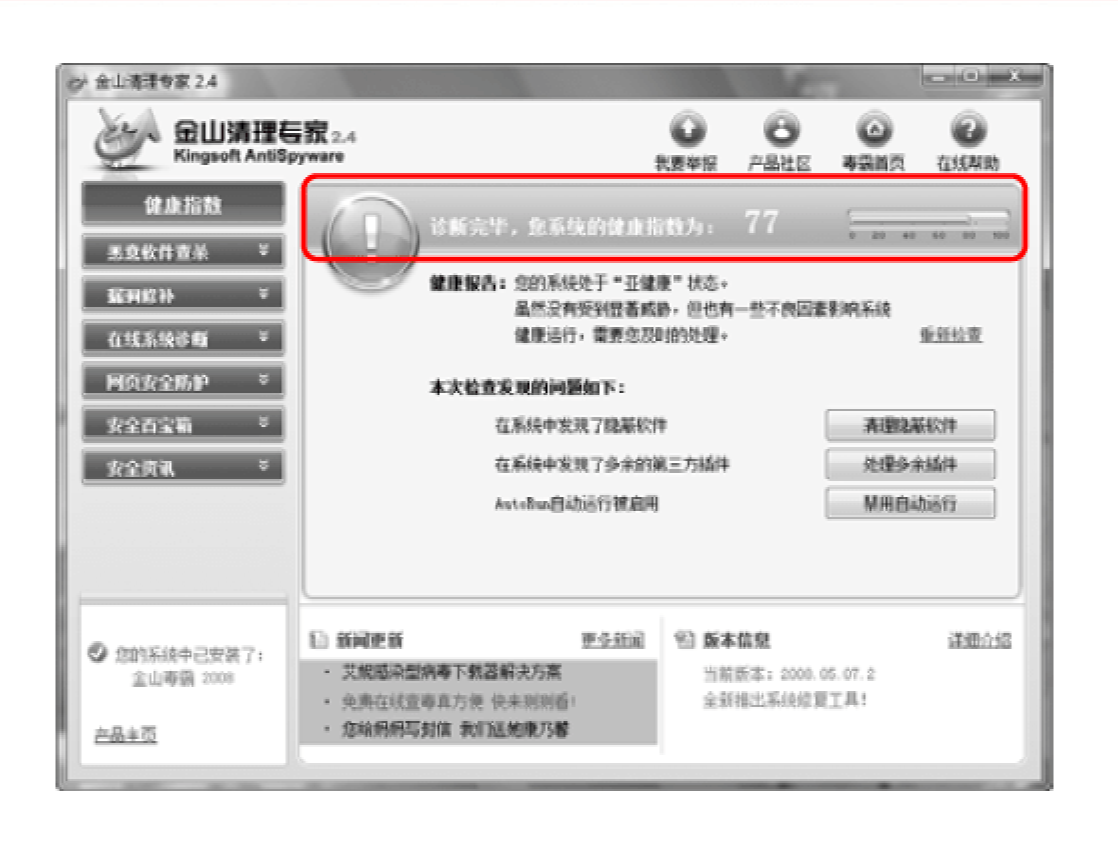
技巧239　利用金山毒霸检查系统的健康指数

金山清理专家检测健康指数的功能可以给系统的健康状况打分，分析系统是否存在安全风险，推荐安全有效的清理方案。

❶ 双击“金山清理专家”图标，进入程序运行主界面。







技巧240　使用金山清理专家查杀系统恶意软件

金山清理专家拥有增强的恶意软件查杀引擎，能彻底查杀 600 多种恶意软件、广告软件，还能隐蔽软件。

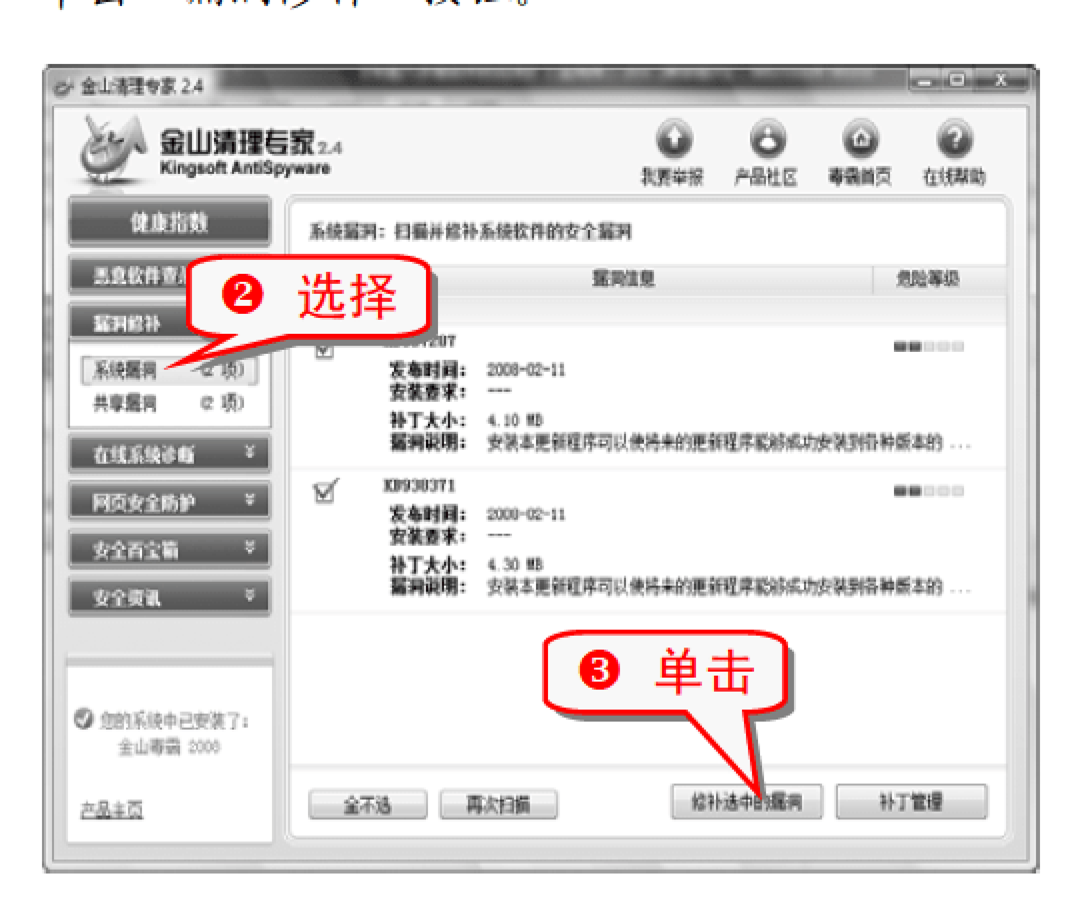
❶ 双击“金山清理专家”图标，进入程序运行主界面，单击“恶意软件查杀”按钮。



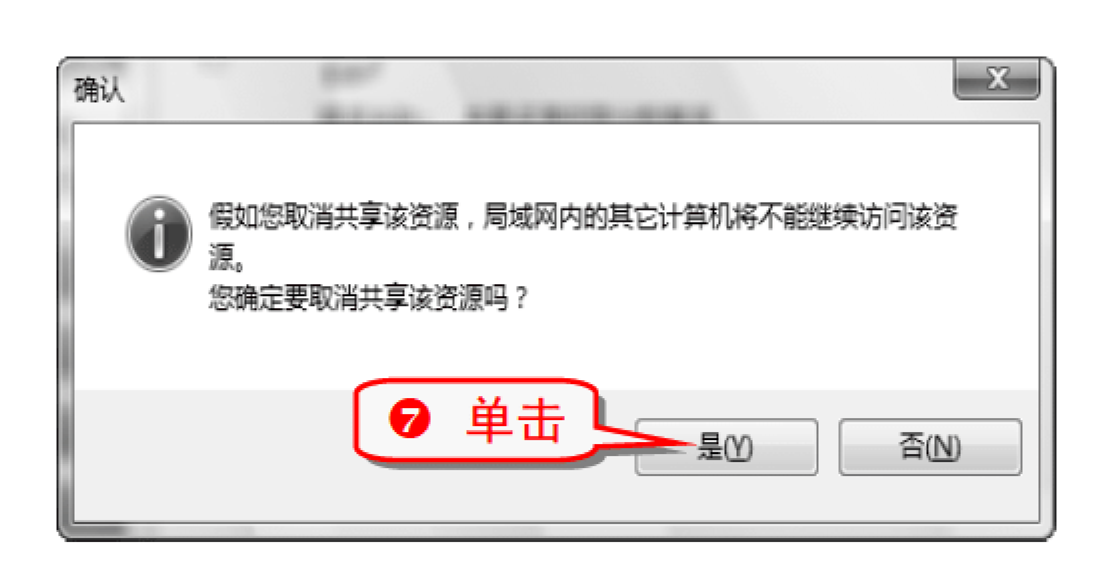
技巧241　使用金山清理专家修补漏洞

金山清理专家的漏洞修补功能可以快速修复操作系统和应用程序漏洞，检查共享漏洞。

❶ 双击“金山清理专家”图标，进入程序运行主界面，单击“漏洞修补”按钮。







技巧242　使用金山清理专家进行在线系统诊断

金山清理专家的在线诊断功能可以全面修复 IE 插件和扩展功能，调整系统启动项，加速电脑启动过程；全面诊断系统，联机自动分析未知加载项。

❶ 双击“金山清理专家”图标，进入程序运行主界面，单击“在线系统诊断”按钮。



❸ 在右窗格中根据需要禁用不必要的启动项，或者右击启动项将其清除。



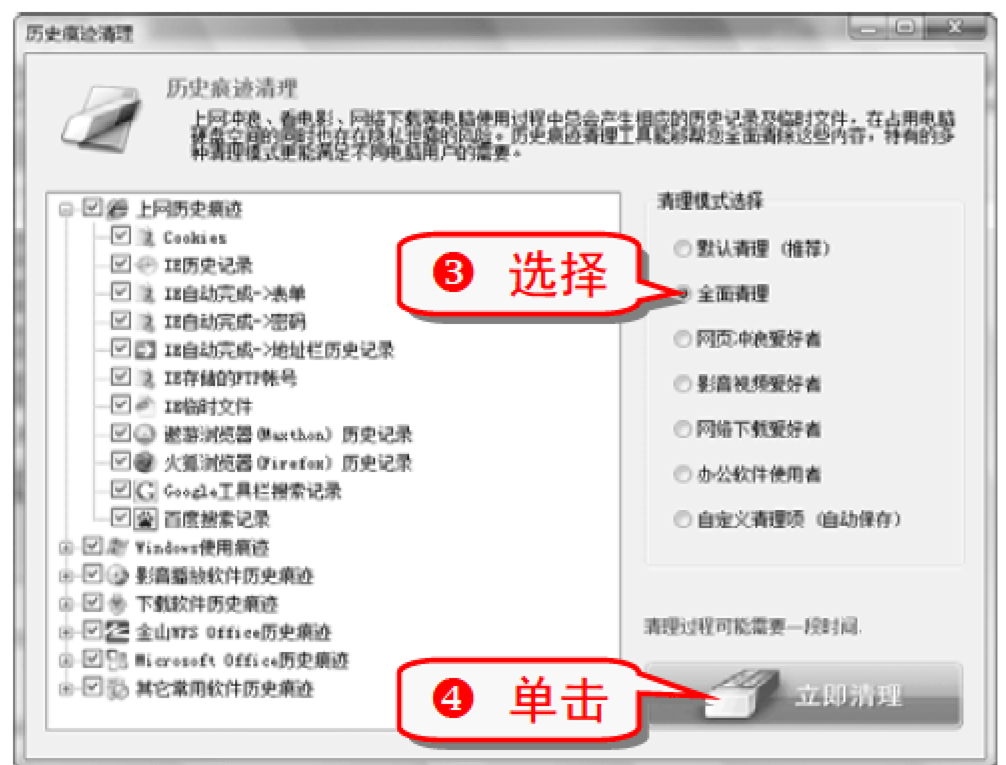


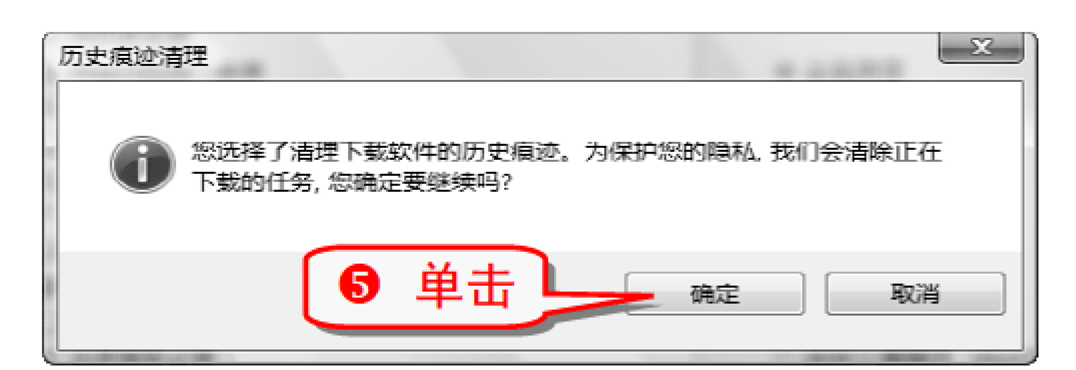
技巧243 使用金山清理专家清理历史痕迹

金山清理专家的历史痕迹清理工具可以全面清理历史使用痕迹，避免历史记录被泄露。

❶ 双击“金山清理专家”图标，进入程序运行主界面，单击“安全百宝箱”按钮。







技巧244 使用金山清理专家清理垃圾文件

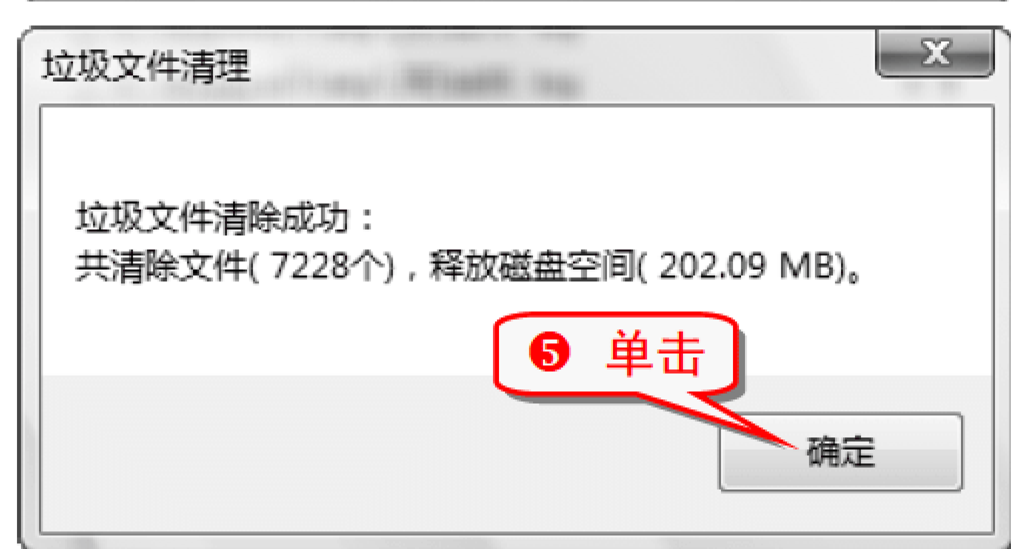
金山清理专家的垃圾文件清理功能，能删除垃圾文件，提高系统性能，回收浪费的磁盘空间。

❶ 双击“金山清理专家”图标，进入程序运行主界面，单击“安全百宝箱”按钮。









技巧245　使用金山清理专家修复系统

金山清理专家的系统修复工具能对系统进行强力修复，消除病毒、木马及恶意软件恶意篡改带来的影响。

❶ 双击“金山清理专家”图标，进入程序运行主界面，单击“安全百宝箱”按钮。

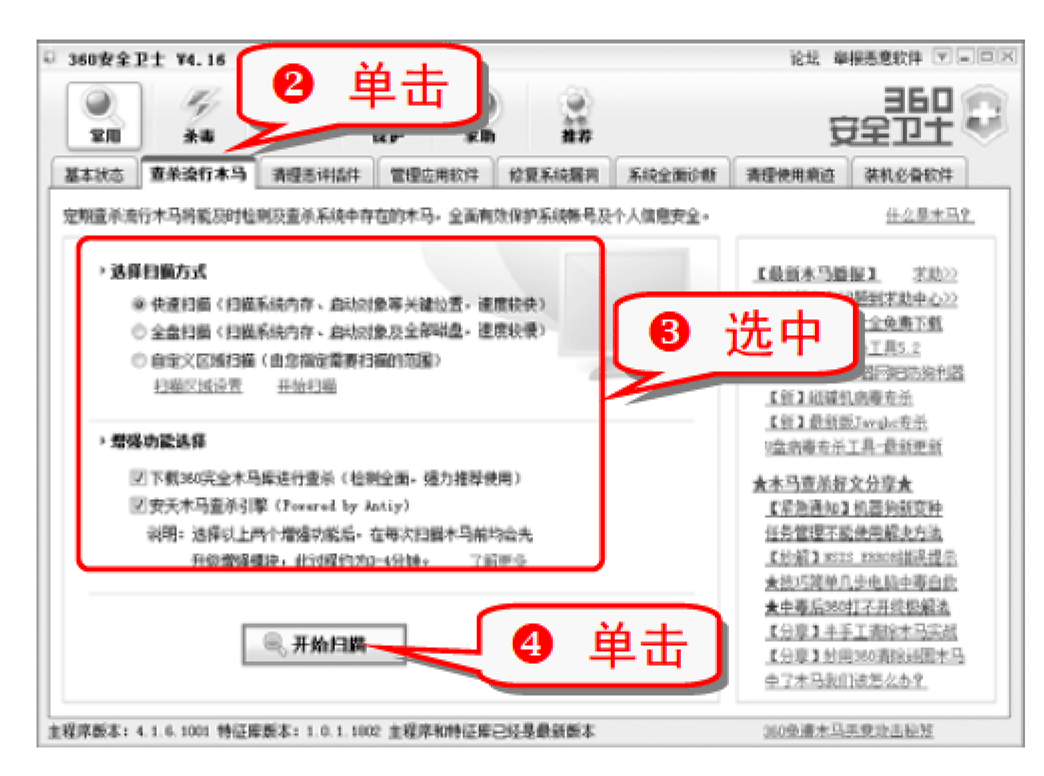




技巧246　使用360安全卫士查杀流行木马

360安全卫士是比较受欢迎的免费安全软件，拥有查杀流行木马、清理恶评插件以及修复系统漏洞等功能，为系统提供全方位的安全保护。

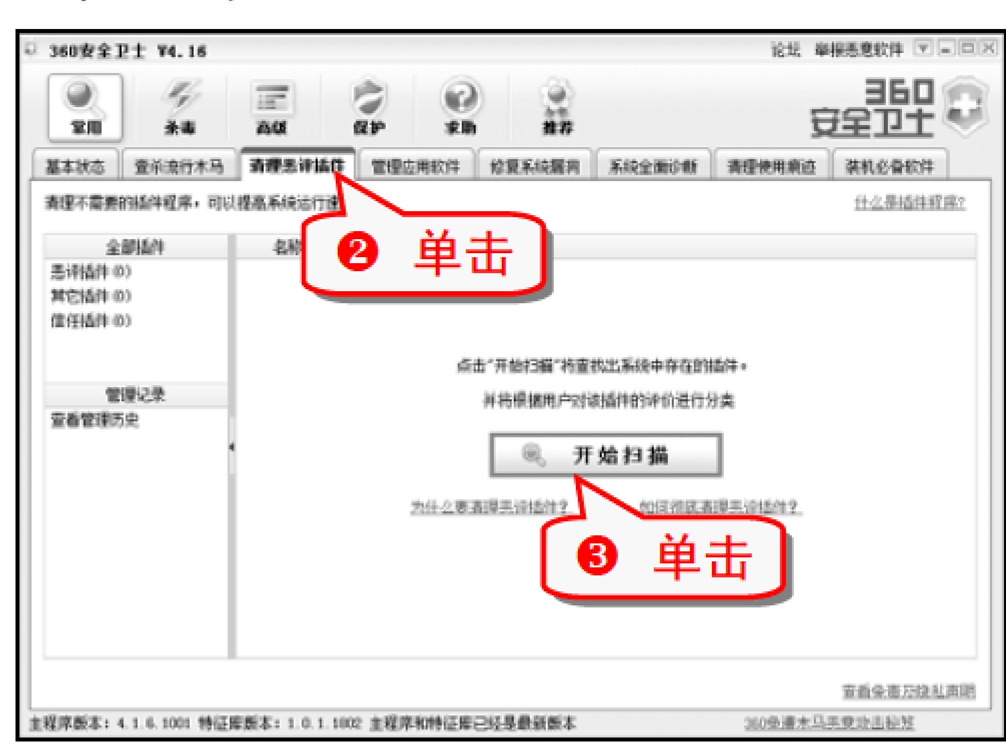
❶ 运行360安全卫士。

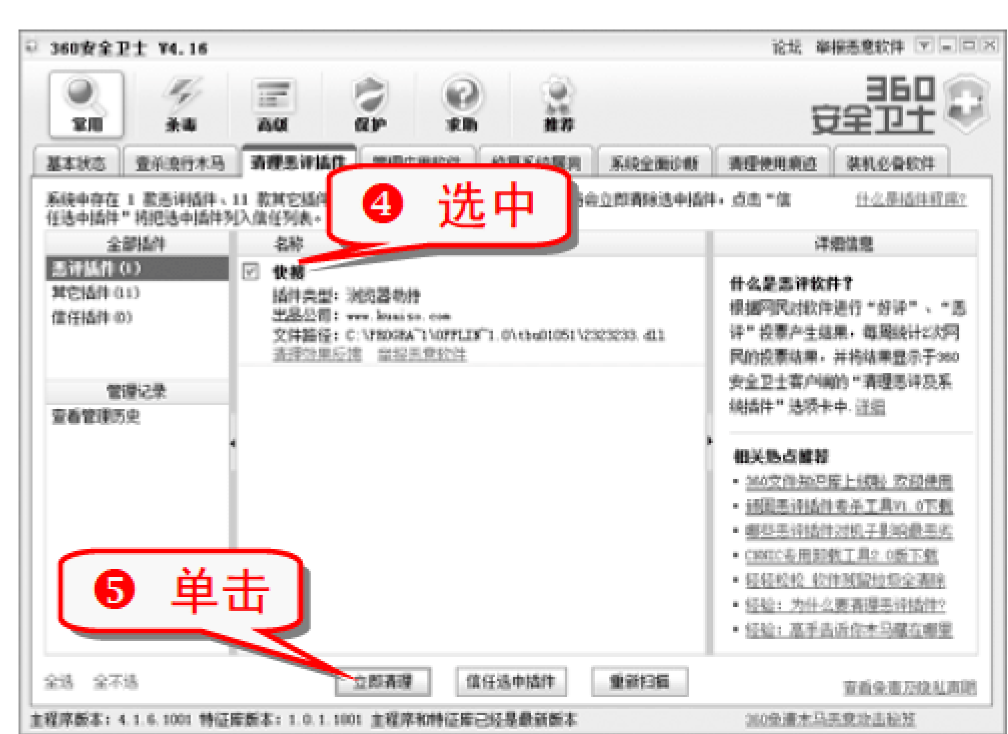


技巧247　使用360安全卫士清理恶评软件

360安全卫士拥有清理恶评软件的功能，能快速查出系统中存在的恶评软件，并将其快速清除。

❶ 运行360安全卫士。



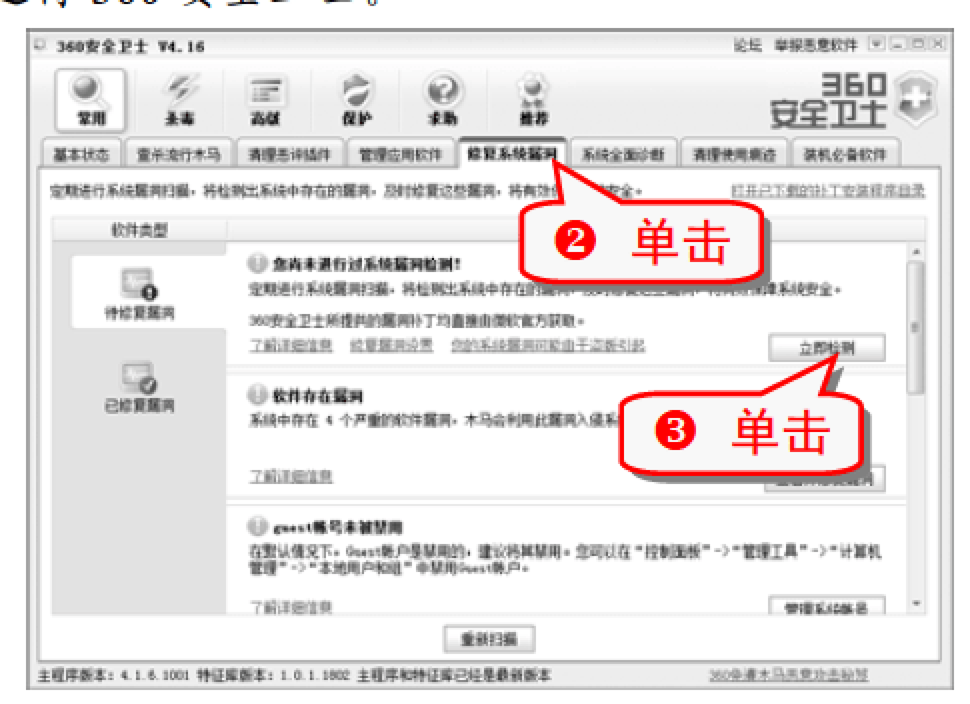


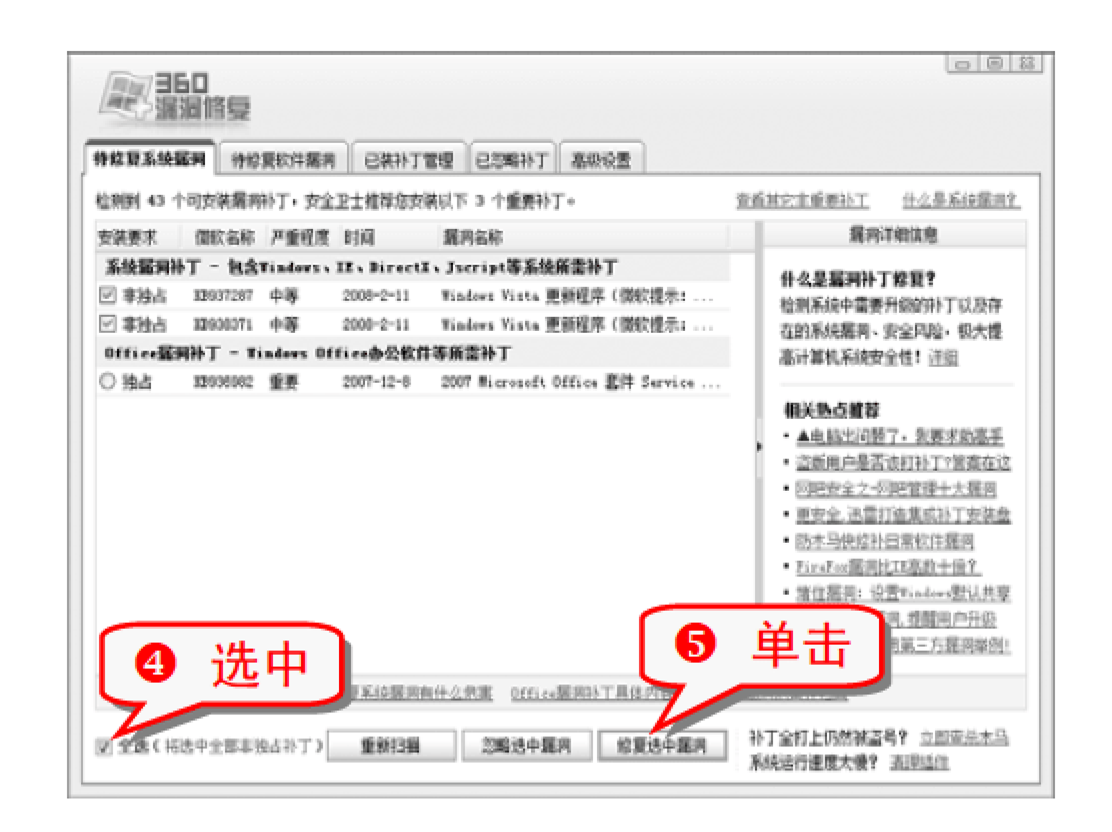


技巧248 使用360安全卫士修复系统漏洞

360安全卫士拥有修复系统漏洞的功能，能快速查出系统中存在的漏洞，提供漏洞下载功能，快速修复系统漏洞。

❶ 运行360安全卫士。





技巧249 使用360安全卫士修复软件漏洞

360安全卫士拥有修复软件漏洞的功能，能快速查出系统中存在的软件漏洞，并将其修复。

❶ 运行360安全卫士。





技巧250 使用360安全卫士修复IE

360安全卫士提供快捷、安全的智能修复方式，快速修复IE中存在的问题。

❶ 运行360安全卫士。



技巧251 使用瑞星杀毒软件查杀病毒

瑞星杀毒软件2008版预先进行了合理的默认设置，在通常情况下无须改动任何设置即可进行病毒查杀。

❶ 启动瑞星杀毒软件。



 举 一 反 三 

右击要杀毒的文件，在弹出的快捷菜单中选择“瑞星杀毒”命令，即可启动瑞星杀毒软件对此文件进行病毒查杀。

用鼠标将要杀毒的文件拖放到桌面上的“瑞星杀毒软件”快捷方式图标上也能对文件进行病毒查杀。

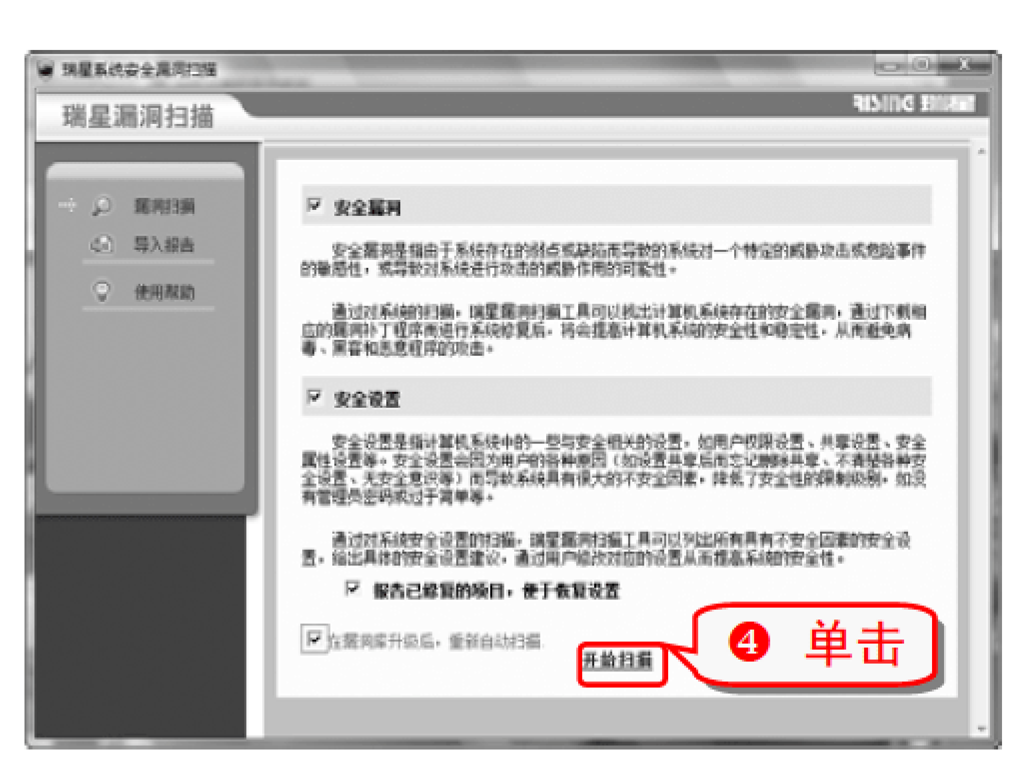
将要杀毒的文件拖放到瑞星杀毒软件主程序窗口中，即可调用瑞星杀毒软件对其进行病毒查杀。

技巧252　使用瑞星杀毒软件对电脑进行安全检查

对电脑进行安检可以为电脑提供全面的检测日志，了解电脑的安全等级及系统状态。

❶启动瑞星杀毒软件。









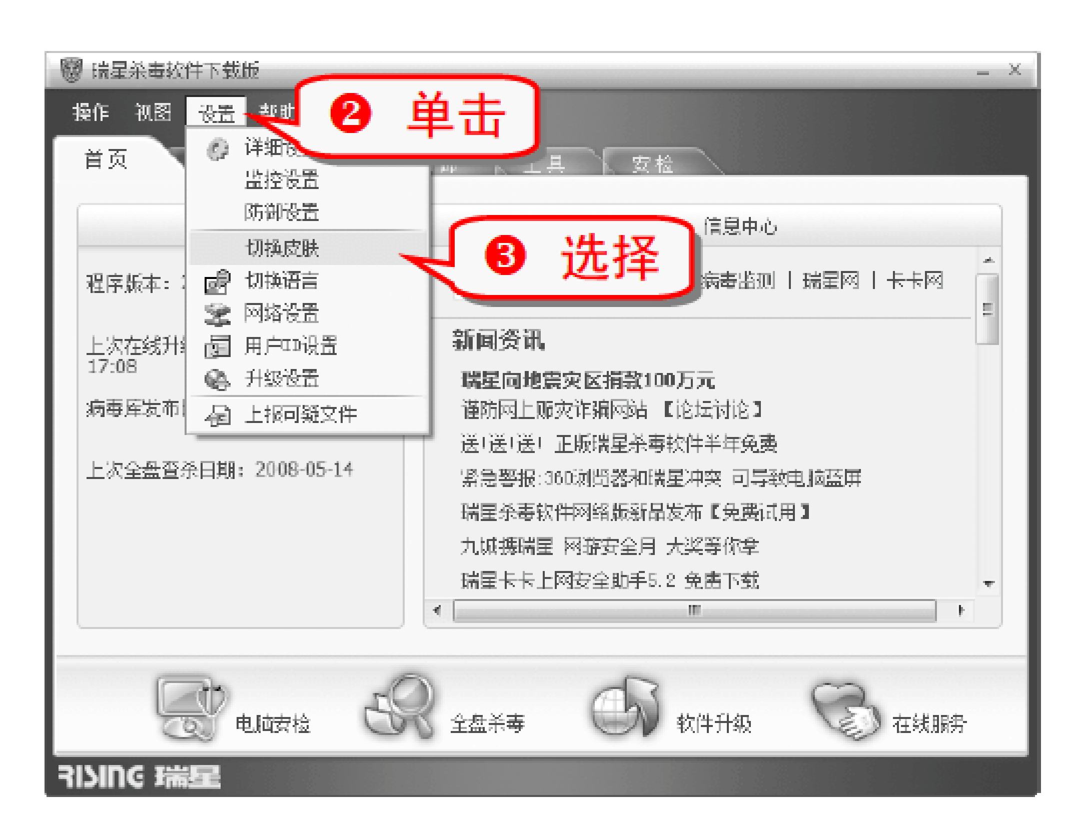
注 意 事 项 

“没有禁用来宾帐号”和“密码的最小长度限制过短”这两个安全设置必须通过手动的方式进行修复。

技巧253　更换瑞星杀毒软件界面的皮肤

瑞星杀毒软件程序界面的皮肤风格包括：怀旧情调、蓝色月光、玄之魅影以及古典朱红。程序默认的皮肤风格是蓝色月光。

❶ 启动瑞星杀毒软件。







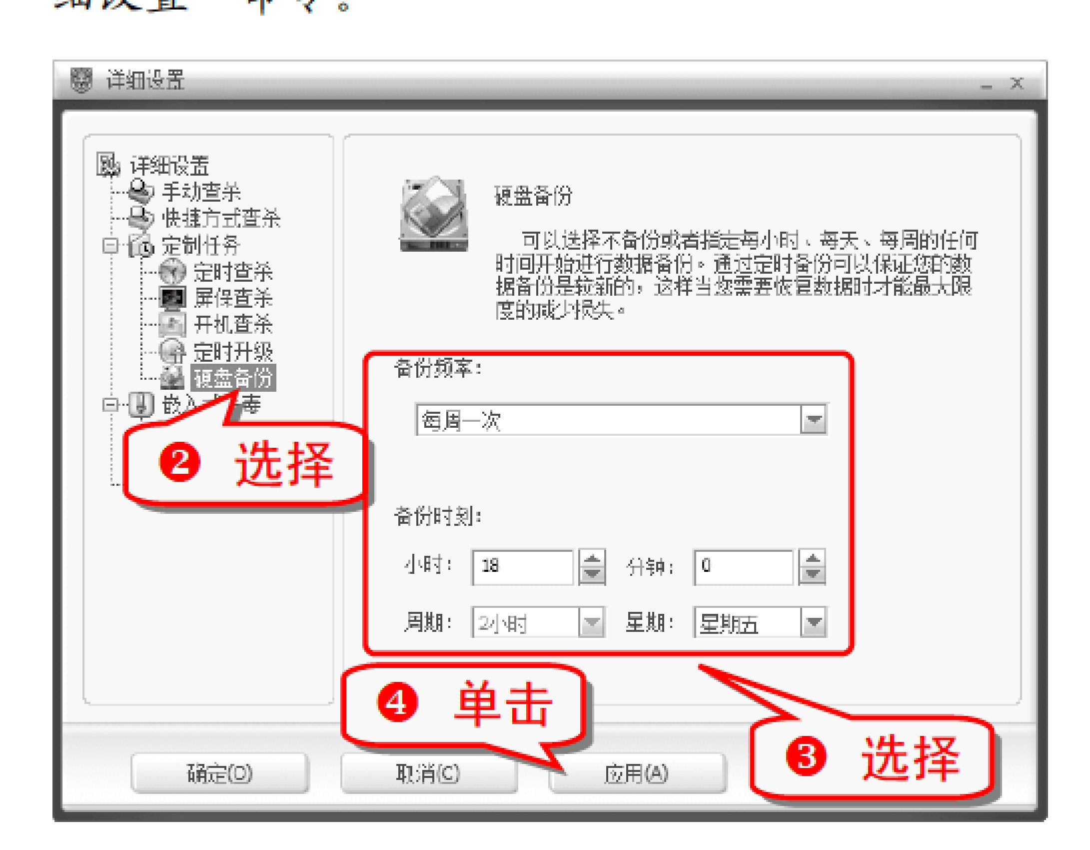
举 一 反 三

更换杀毒软件界面语言的方式与更换皮肤的方式类似。

技巧254 使用瑞星杀毒软件备份硬盘数据

瑞星硬盘数据备份功能，只备份整个硬盘的重要信息，与系统自带的系统还原功能有很大的差别。

❶ 在瑞星杀毒软件主程序界面中，选择“设置”→“详细设置”命令。







技巧255 使用瑞星杀毒软件还原硬盘数据

瑞星杀毒软件的硬盘数据恢复功能，可以恢复硬盘中被破坏的数据，但是必须先使用瑞星数据备份工具备份硬盘数据。

❶ 将电脑的启动顺序设为首先从光盘启动。

❷ 将瑞星杀毒软件 2008 版光盘放入光驱。

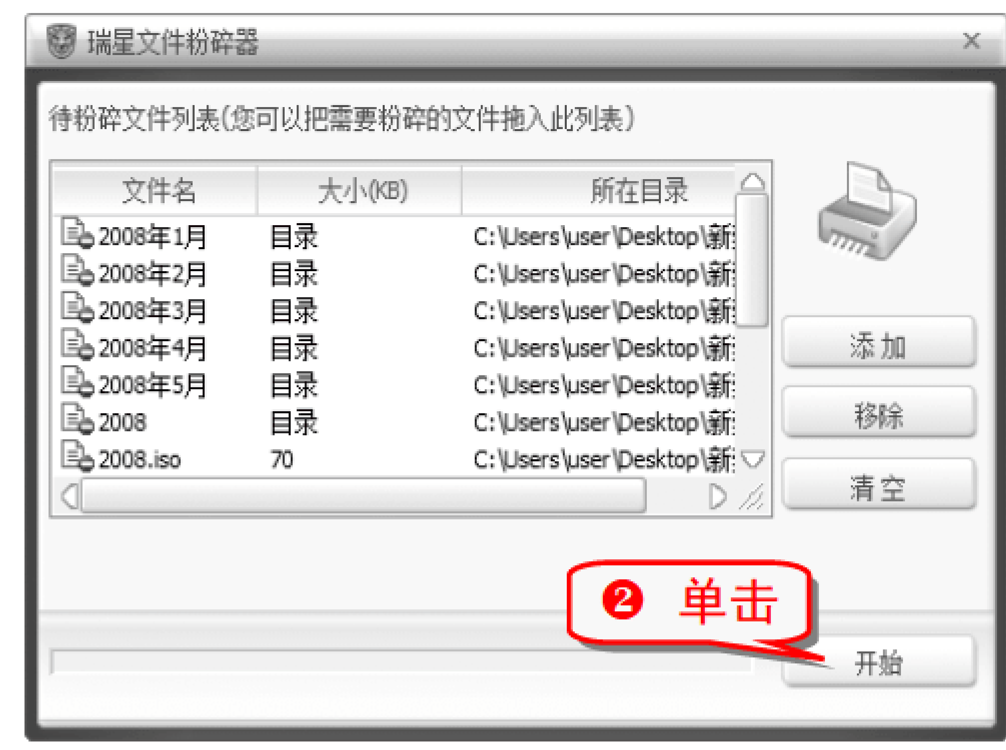
❸ 重新启动电脑，使系统自动从光盘启动。

❹ 进入瑞星杀毒主界面，单击“恢复”按钮即可恢复硬盘数据。

技巧256 使用瑞星杀毒软件粉碎文件

瑞星杀毒软件的文件粉碎功能可以将文件数据完全粉碎，并且无法用常规手段恢复，可以保证隐秘资料的安全。

❶ 右击需要粉碎的文件，在弹出的快捷菜单中选择“粉碎文件”命令，弹出“瑞星文件粉碎器”对话框。





注 意 事 项

粉碎文件的操作将导致被粉碎的文件无法恢复，在进行粉碎操作的时候切勿大意，否则会造成难以挽回的损失。

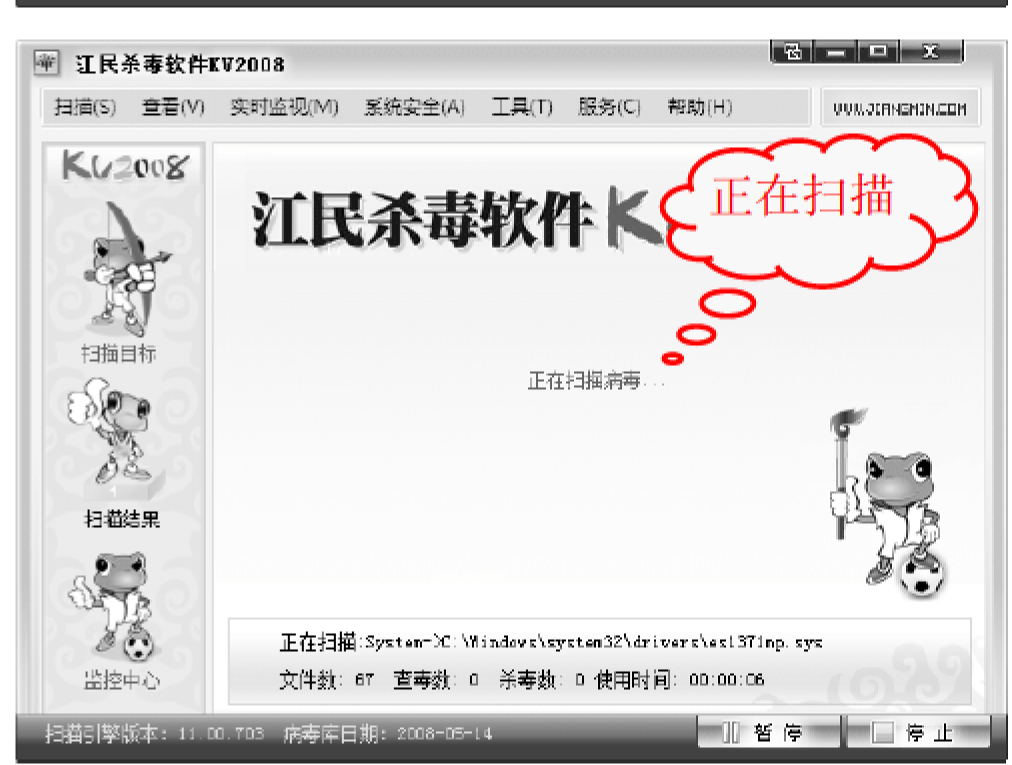


技巧257　使用江民杀毒软件扫描病毒

江民杀毒软件 KV2008 采用新一代智能分级高速杀毒引擎，占用系统资源少，扫描速度快。

❶ 运行江民杀毒软件主界面。



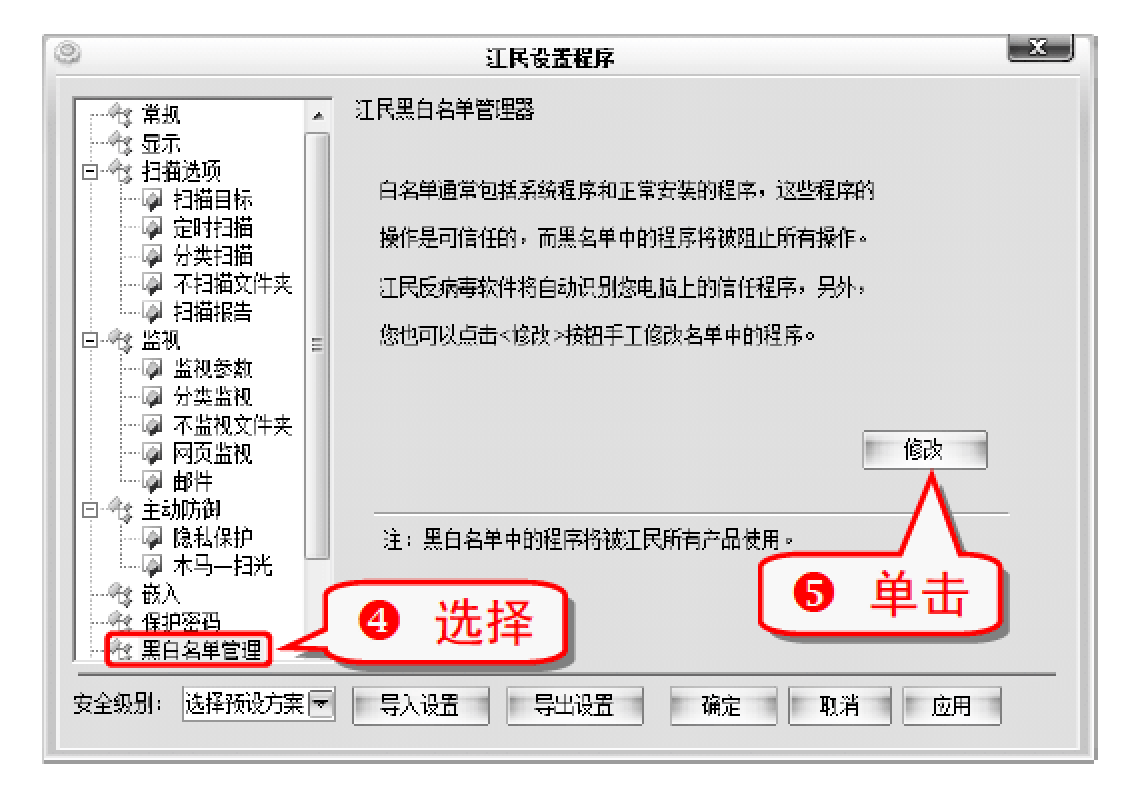


技巧258　使用江民杀毒软件管理黑白名单

通过黑白名单管理功能可以阻止非法程序的运行。

❶ 运行江民杀毒软件主界面。



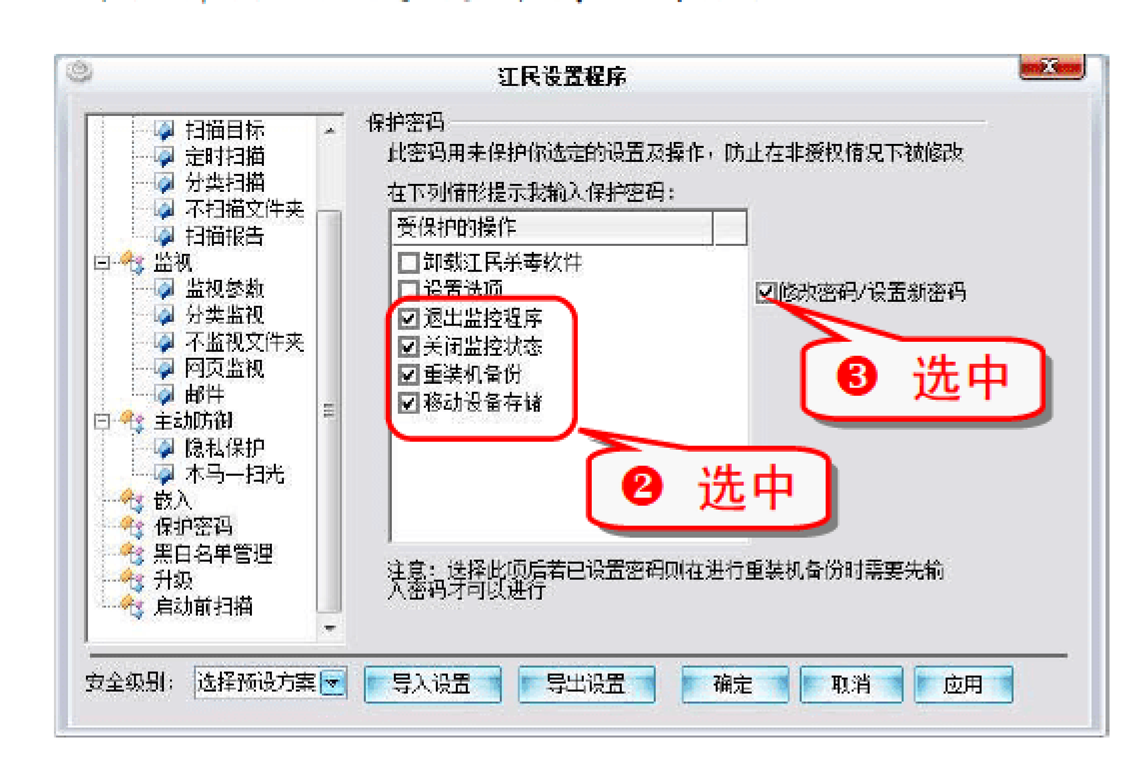


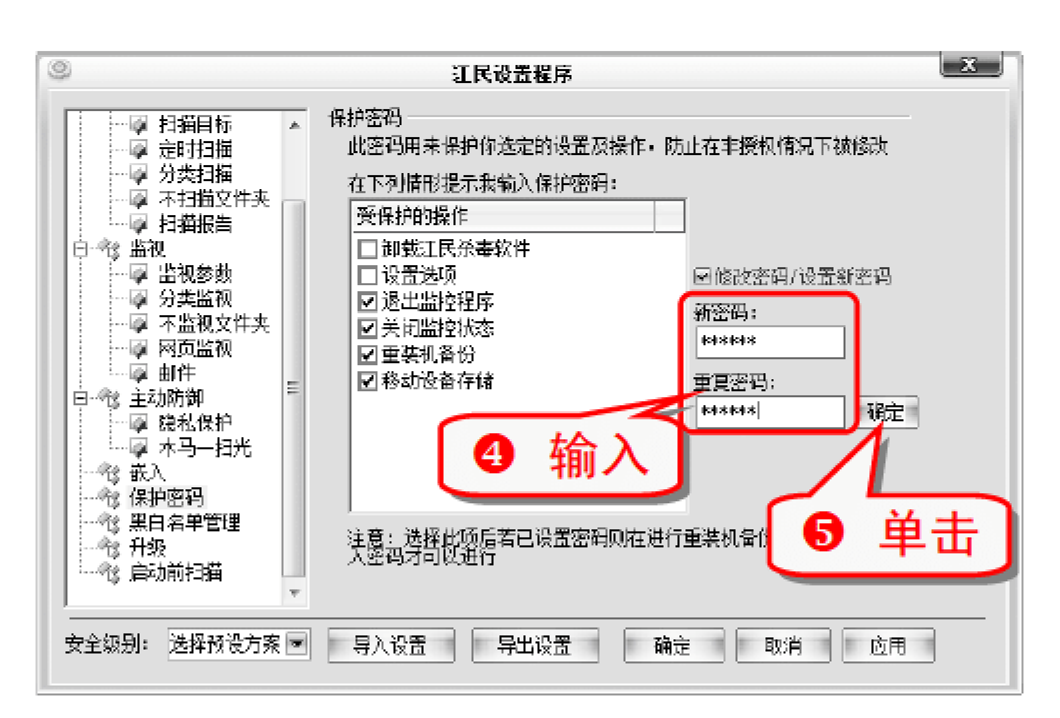


技巧259　为江民杀毒软件设置保护密码

设置保护密码可以防止黑客非法修改选定的设置以及操作。

❶ 在江民杀毒软件主界面上选择“工具”→“设置”命令，弹出“江民设置程序”对话框。





技巧260 使用江民杀毒软件管理共享资源

江民杀毒软件的共享管理功能可以查看并删除电脑上的共享对象。

❶ 运行江民杀毒软件主界面。

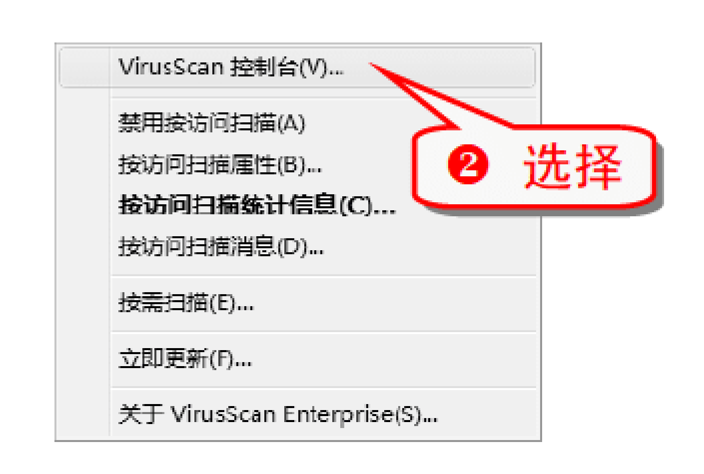


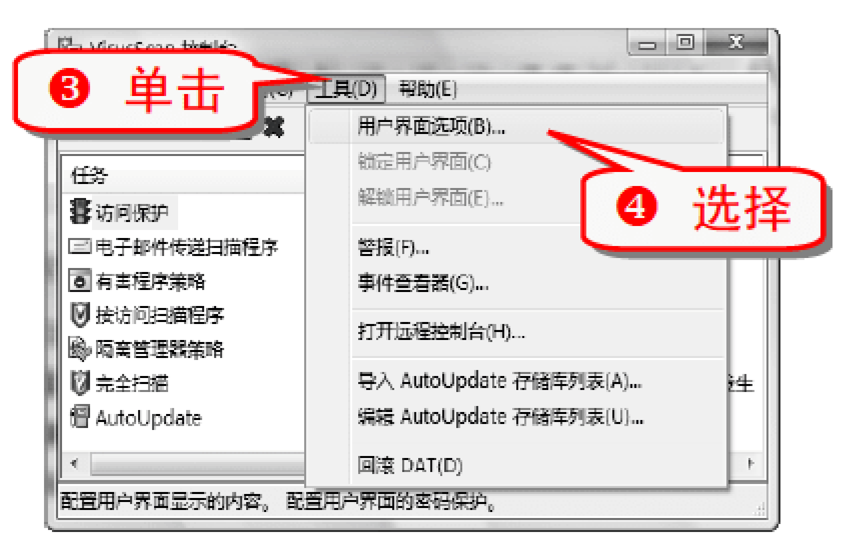


技巧261 保护 McAfee VirusScan Enterprise 用户界面安全

作为管理员可以控制用户对 McAfee VirusScan Enterprise 界面的访问权限。通过指定密码可以防止用户访问或更改选定功能，也可以根据需要锁定和解锁用户界面。

❶ 杀毒软件安装好以后，会在通知区域显示杀毒软件的图标，右击该图标，弹出快捷菜单。







知 识 补 充

弹出的用户界面选项中有“显示选项”和“密码选项”两个选项卡。

- “显示选项”选项卡指定用户可以查看的系统任务栏图标选项，允许连接到远程计算机，配置控制台语言。
- “密码选项”选项卡为整个系统或所选项目指定密码安全。



专 家 坐 堂

设置密码对用户的影响如下。

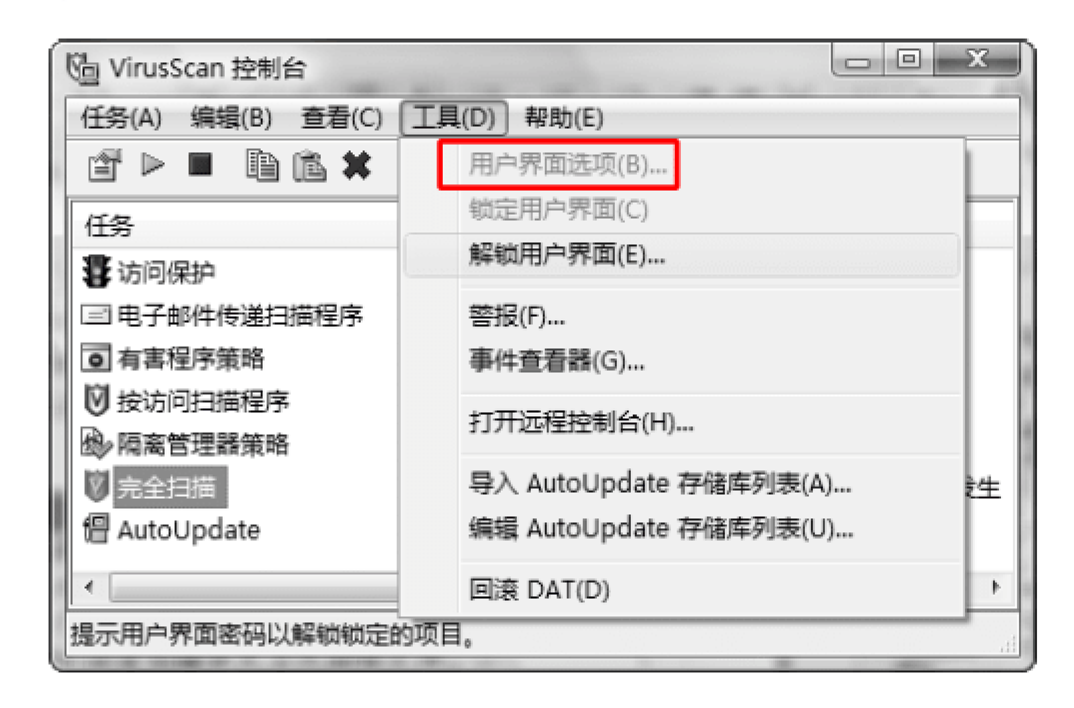
非管理员(无管理员权限的用户)，在只读模式下运行所有 McAfee VirusScan Enterprise 应用程序，可以查看某些配置参数、运行已保存的扫描以及运行即时扫描和更新，但是不能更改任何配置参数，不能创建、删除或修改已保存的扫描或更新任务。

管理员(拥有管理员权限的用户)，输入密码可以在读/写模式下访问受保护的选项卡和控件。如果未提供保护项目的密码，则只能在只读模式下查看。

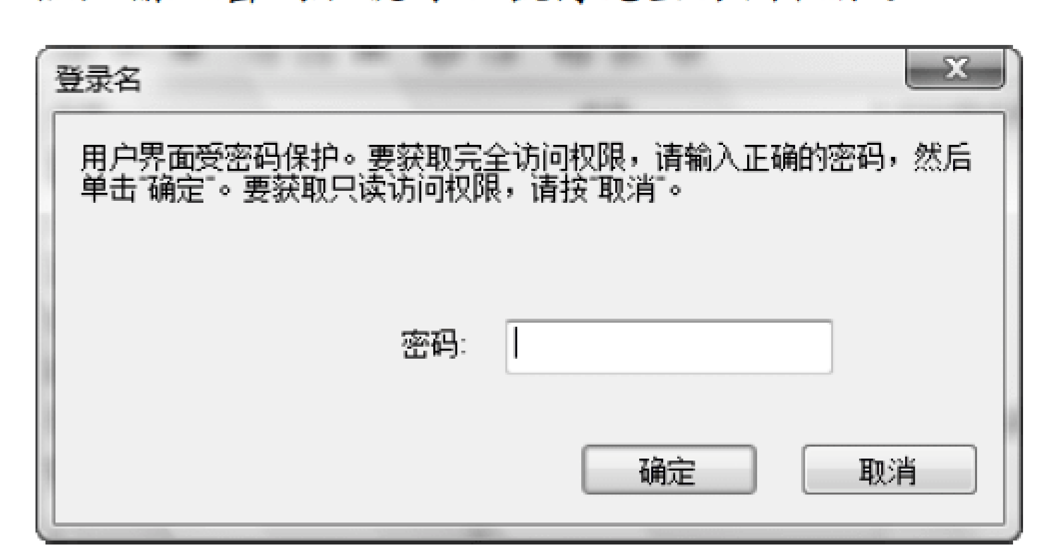




❾ 设置密码保护以后，单击“工具”按钮弹出的下拉菜单中的“用户界面选项”变成灰色。



❿ 选择“解锁用户界面”命令后，弹出“登录名”对话框，输入密码后就可以获得完全访问权限。



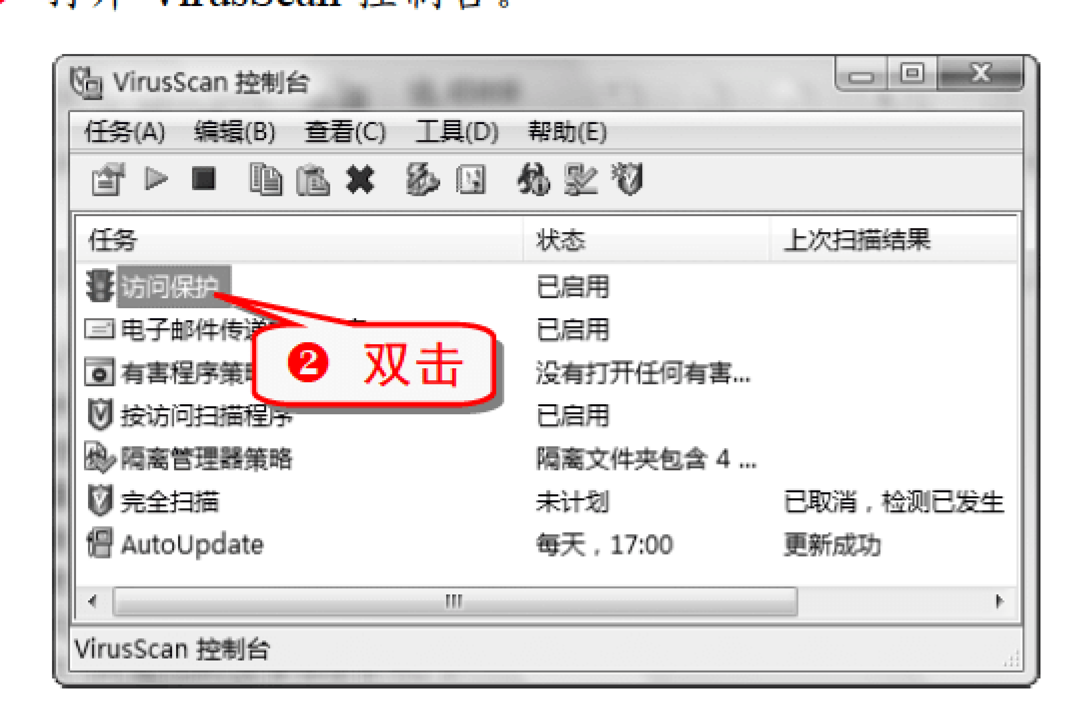
举　一　反　三

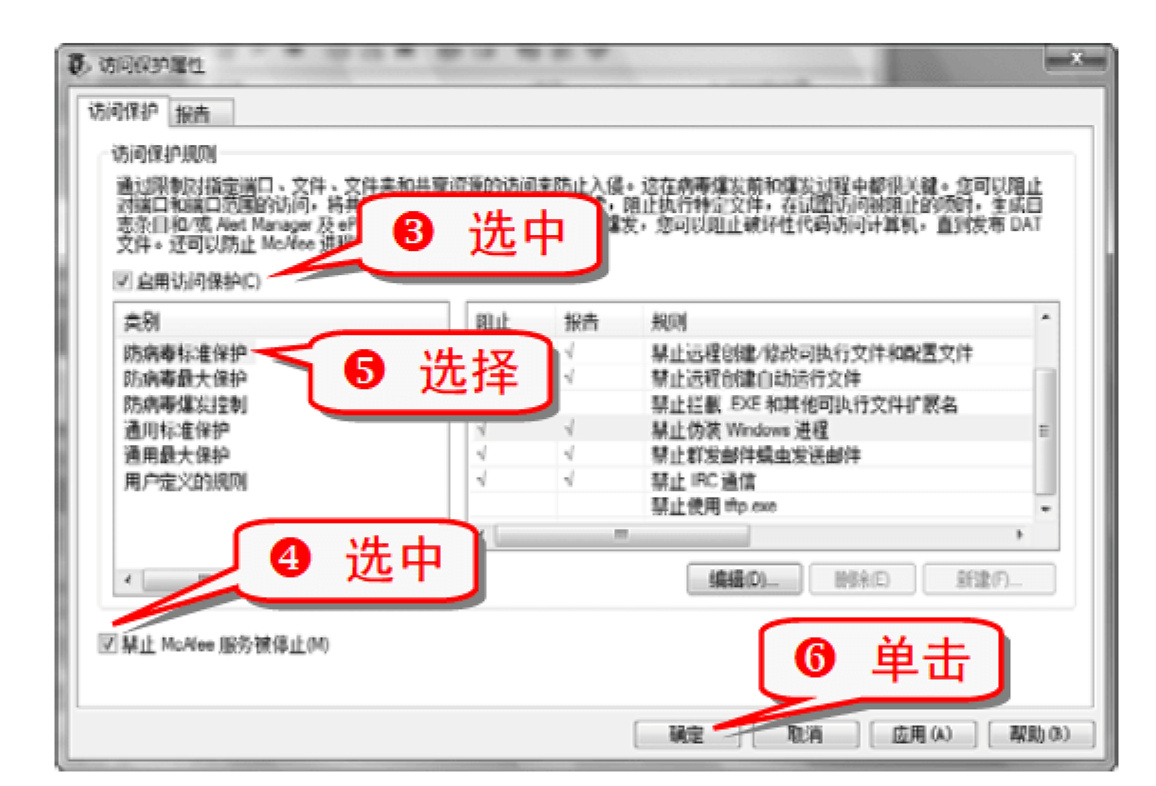
要锁定用户界面，请选择“工具”→“锁定用户界面”命令。

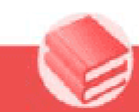
技巧262　设置 McAfee VirusScan Enterprise 访问保护

访问保护通过限制对指定的端口、文件、文件夹、共享资源、注册表项和注册表值的访问来防止对电脑的有害更改。这种保护在病毒爆发前和爆发期间都很关键。

❶ 打开 VirusScan 控制台。







专　家　坐　堂

规则分为以下类别。

防病毒标准保护，保护某些关键设置和文件不被修改，但允许安装和执行合法软件。

防病毒最大保护，保护大多数关键设置和文件不被修改，会禁止安装合法软件。

防病毒爆发控制，在发布 DAT 文件之前，阻挡破坏性代码在爆发期间访问电脑。预配置这些规则后，可以阻挡破坏性代码在爆发期间对共享资源的访问。

通用标准保护，保护某些通用文件和设置不被修改，允许安装和执行合法软件。

通用最大保护，保护大多数通用文件和设置不被修改，同时也会禁止安装合法软件。

用户定义的规则，补充“防病毒”和“通用”规则提供的保护。



注　意　事　项

即使选择了“禁止 McAfee 服务被停止”，具有调试程序权限的用户仍然可以停止 McAfee 进程。

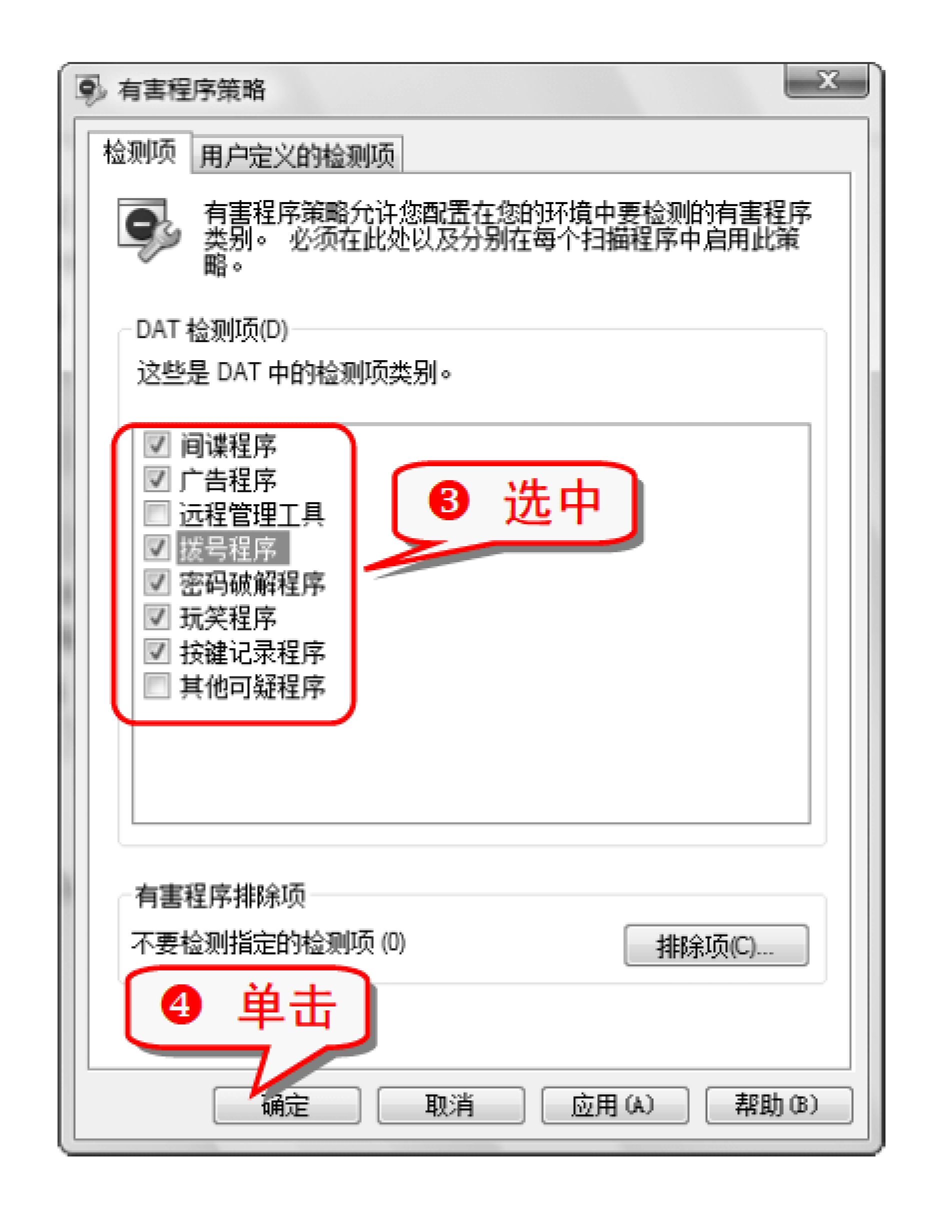
默认情况下，管理员对 Windows 操作系统拥有调试程序权限。从用户权限中删除这些权限，用户将无法停止 McAfee 进程。

技巧263　配置 McAfee VirusScan Enterprise 有害程序策略

McAfee VirusScan Enterprise 能保护电脑免受有害程序的危害。

❶ 打开 VirusScan 控制台。

❷ 在“VirusScan 控制台”中，双击“有害程序策略”选项，打开“有害程序策略”对话框。

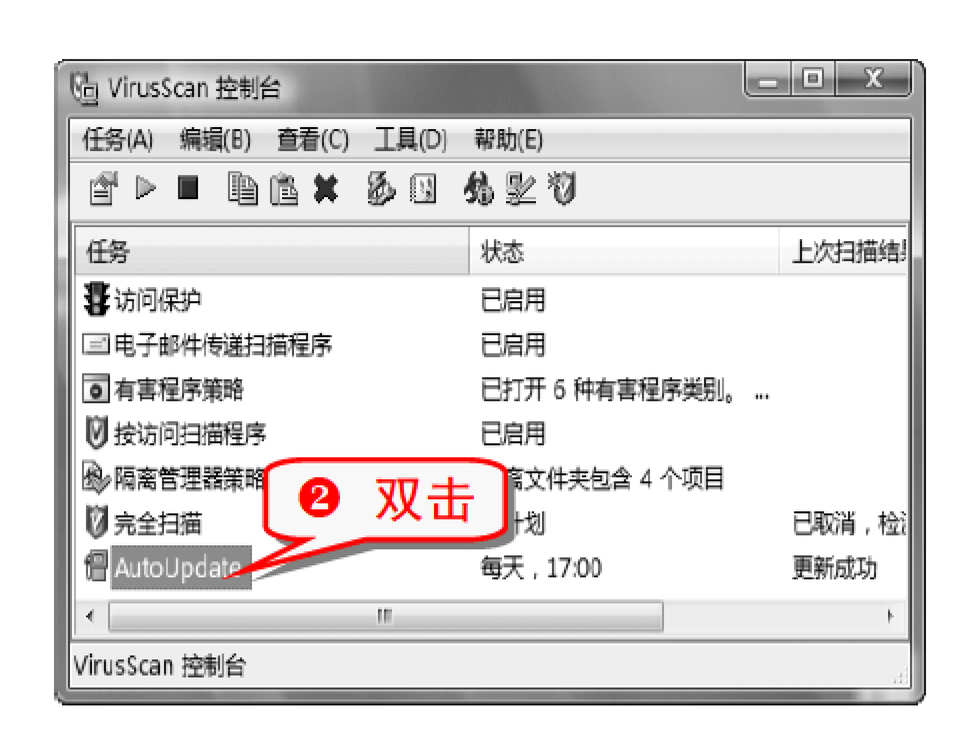




技巧264　为 McAfee VirusScan Enterprise 设置自动更新时间

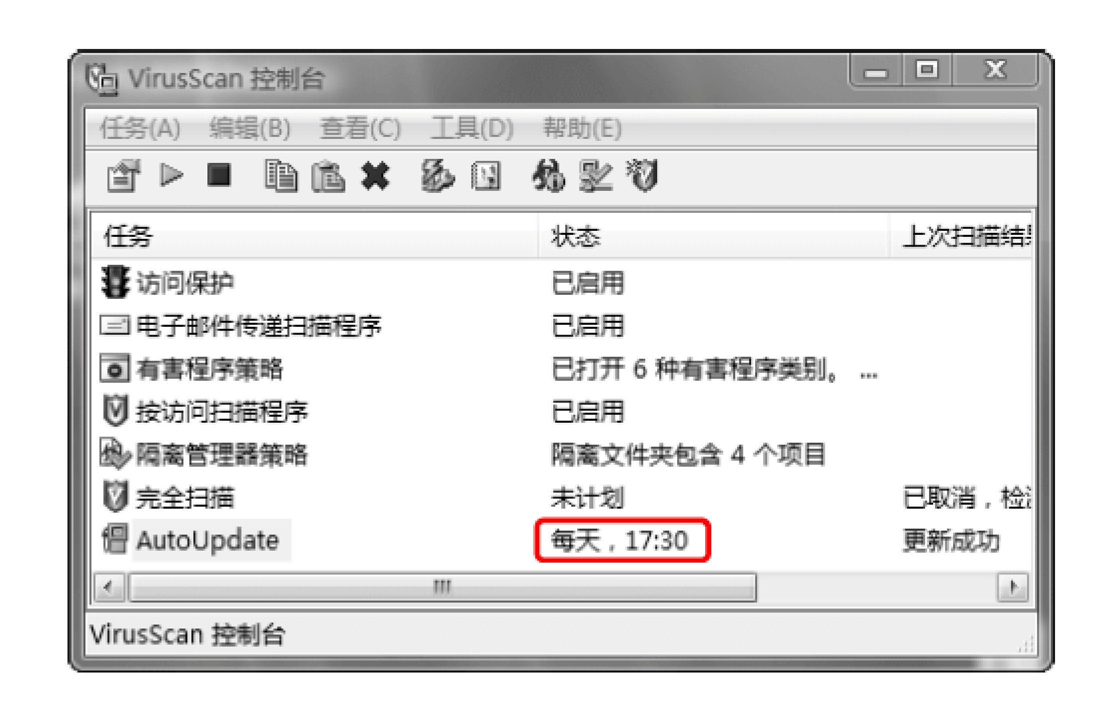
McAfee 每天都结合最新的研究成果，发布新的 DAT 文件。AutoUpdate 功能是使用更新任务，自动检索最新的 DAT 文件、extra.DAT 文件、扫描引擎、产品更新、Service Pack 以及修补程序。

❶ 打开 VirusScan 控制台。





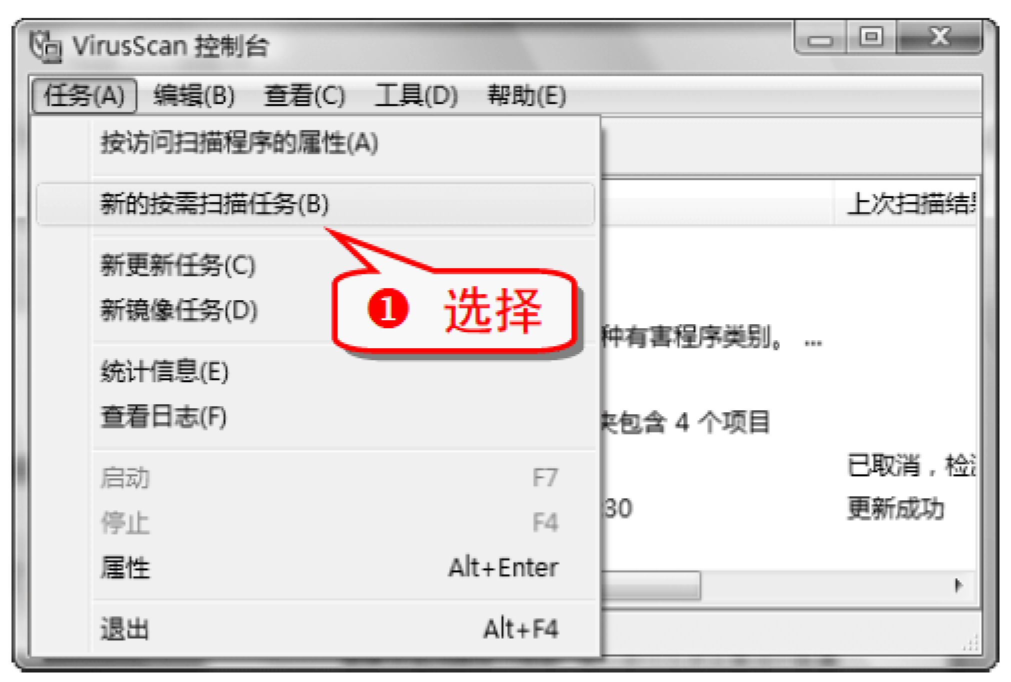


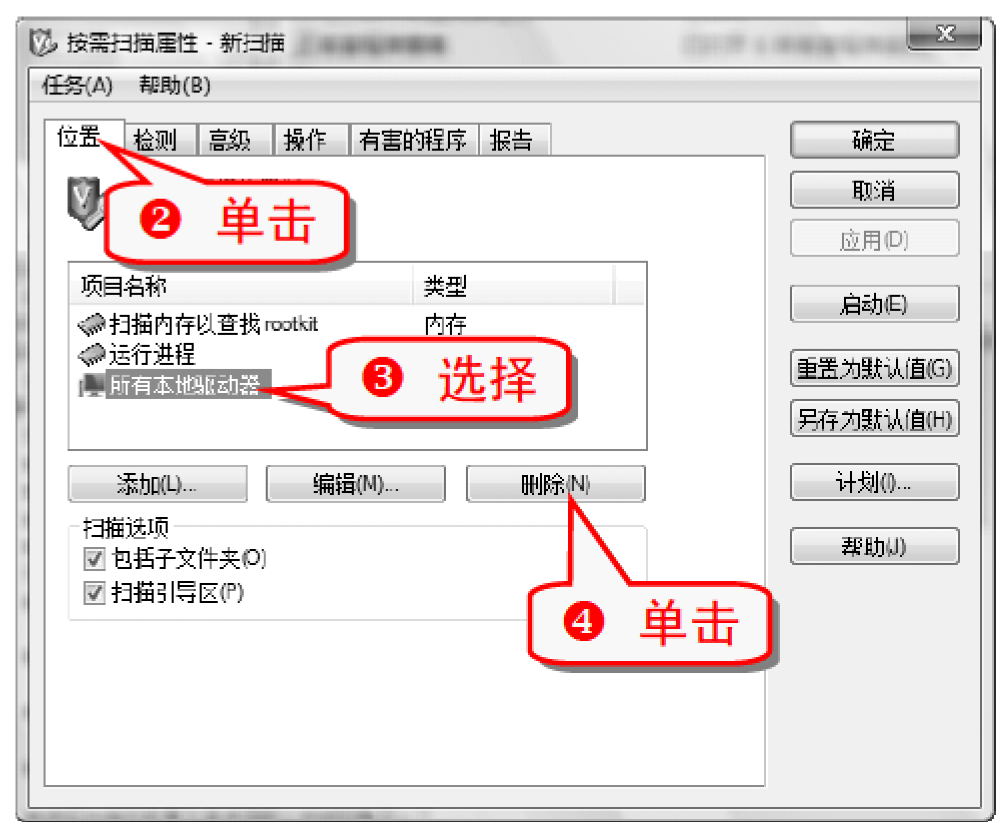


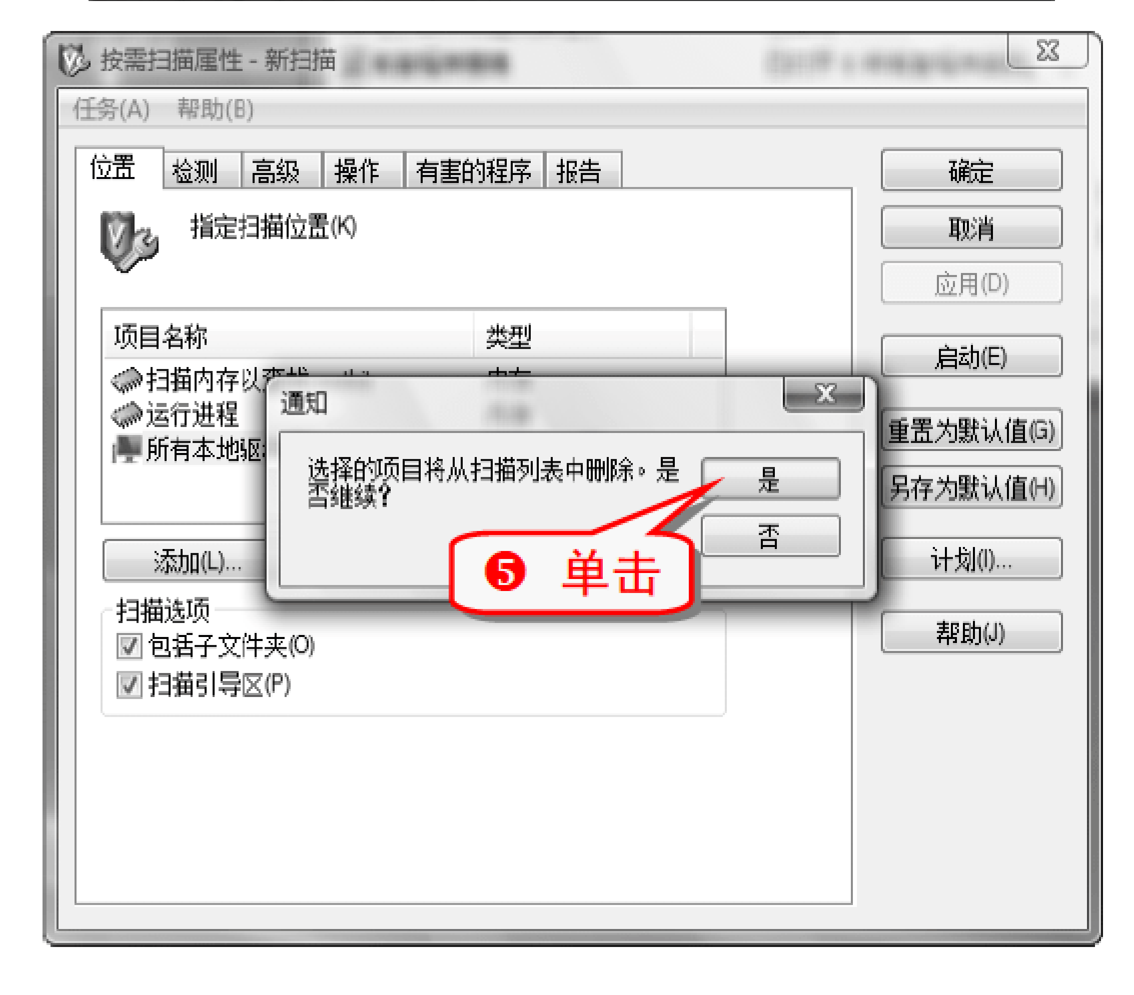


技巧265　新建 McAfee VirusScan Enterprise 按需扫描任务

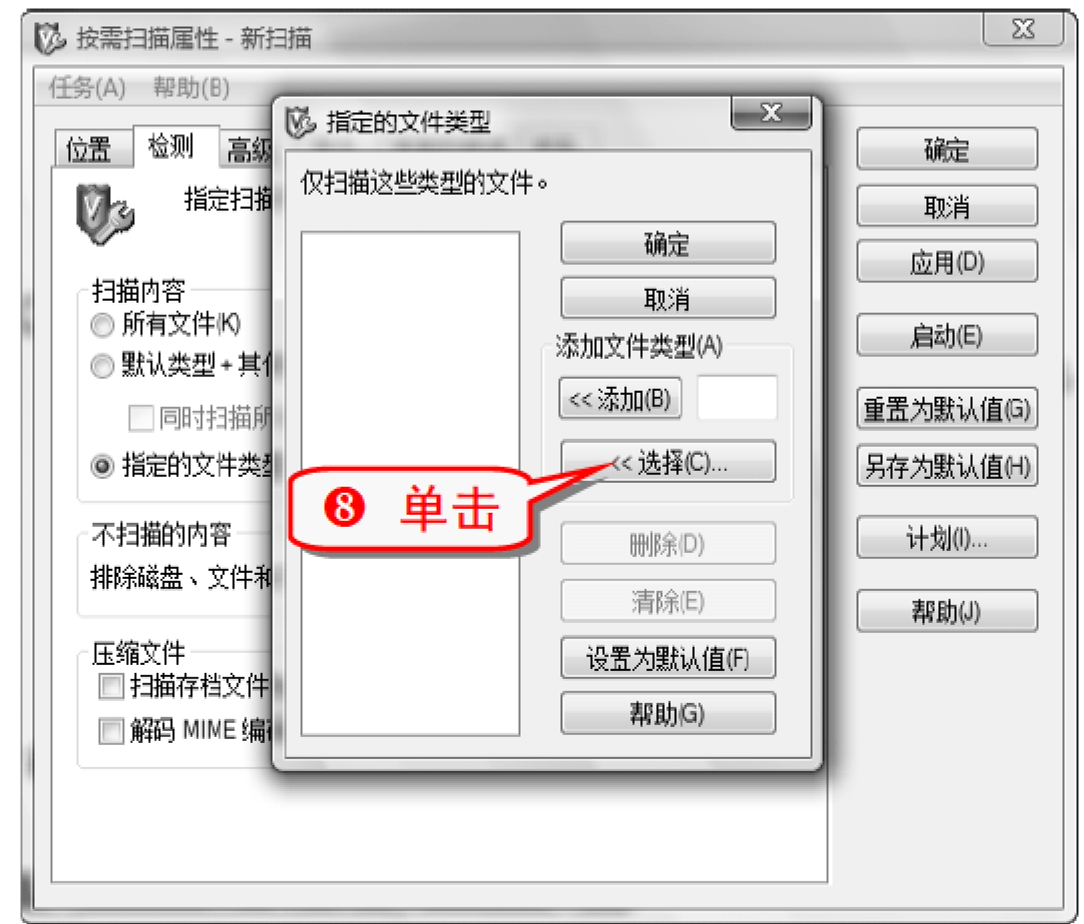
按需扫描程序用于在适宜时间或定期扫描电脑以查找潜在威胁。使用按需扫描可以在不影响工作的情况下计划定期扫描。

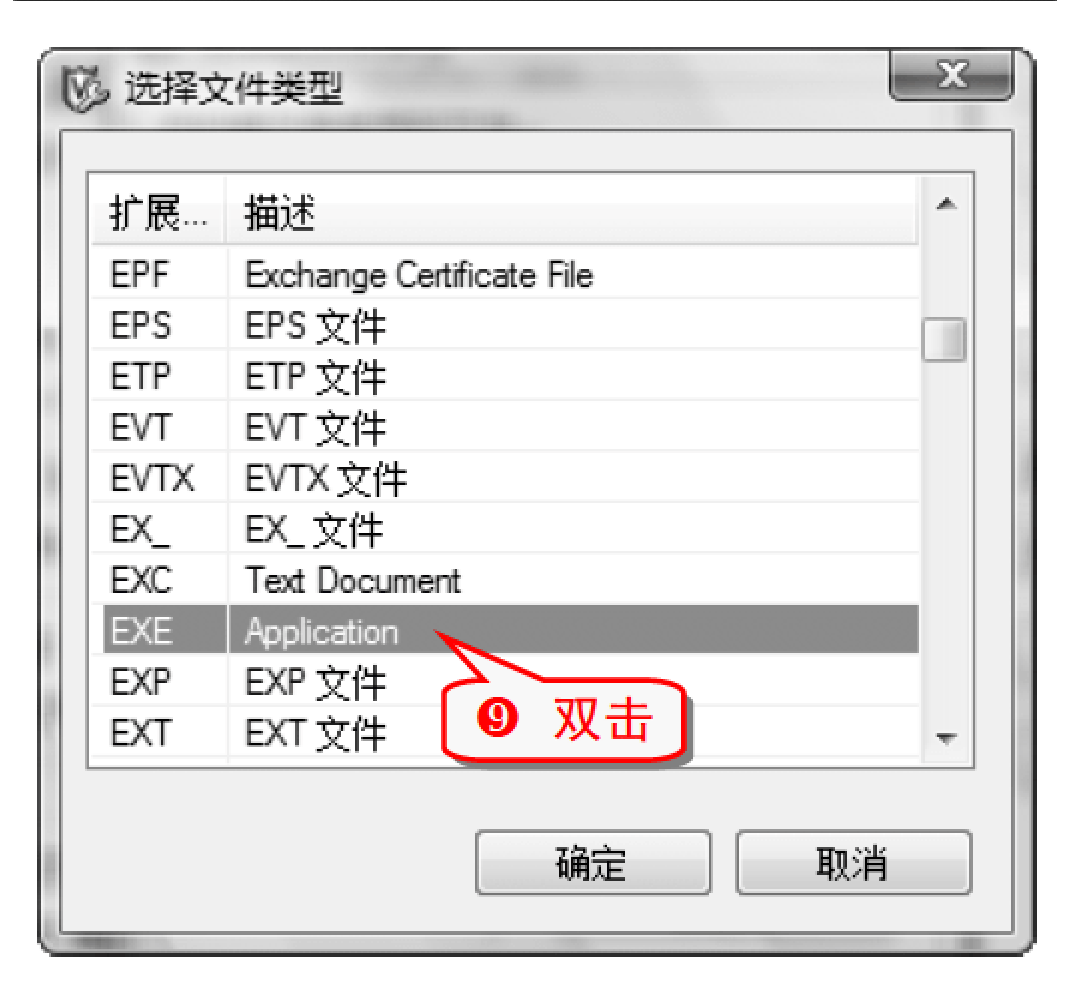


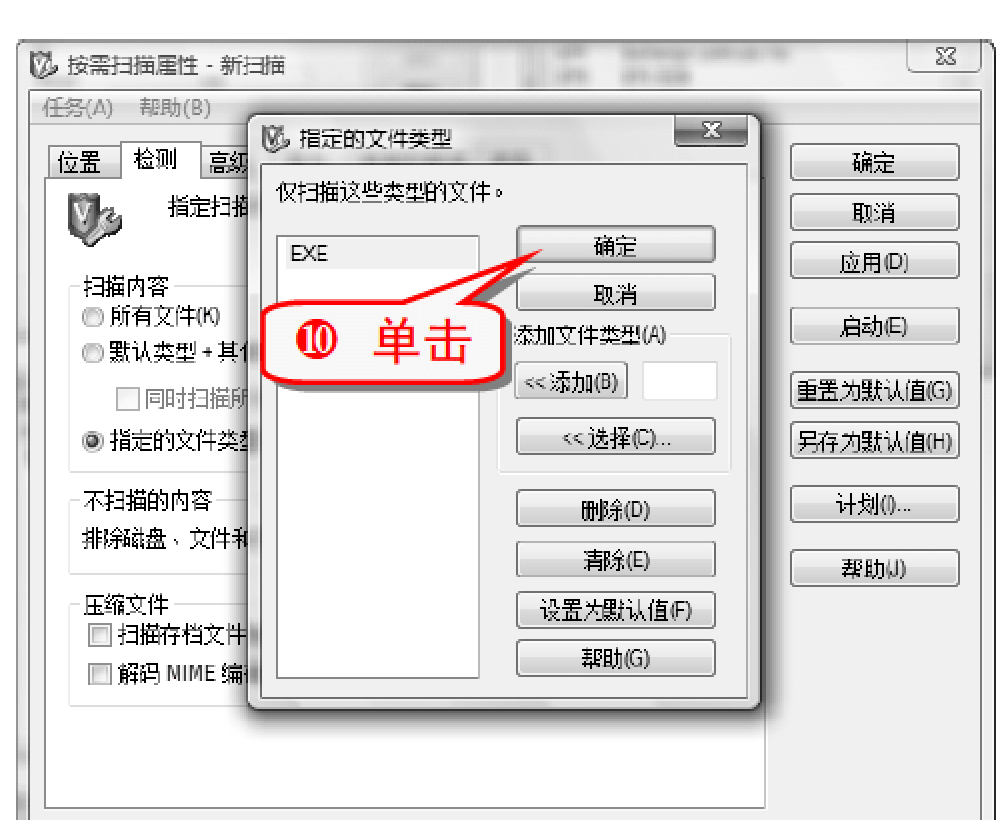












其他的配置只要按默认配置进行设置即可，这样就可以随时扫描那些.exe 文件了。



专题十　防火墙完全攻略

内容导航

装了杀毒软件就不用安装防火墙是一种错误的想法，防火墙是根据连接网络的数据包来进行监控的，可以防御黑客对系统的攻击，而杀毒软件是无法做到这一点的。

热点快报

- 金山网镖
- 瑞星防火墙
- 傲盾防火墙
- 江民防火墙
- 龙盾防火墙
- 360 防火墙

技巧266　金山网镖 2008

金山网镖 2008 属于网络防火墙，能防御一般的网络攻击，可以保障上网安全。

金山网镖 2008 的主界面有操作、工具、窗口以及帮助四个不同功能的菜单栏按钮。



技巧267　金山网镖 2008 的“操作”菜单

金山网镖 2008 的“操作”菜单下有“断开网络”、“开机自动运行”和“退出”3 个功能。



- 选择“操作”→“断开网路”命令，断开网络连接。
- 选择“操作”→“恢复网路”命令，恢复网络连接。
- 选择“操作”→“开机自动运行”命令，使系统启动后自动启用金山网镖 2008。
- 选择“操作”→“退出”命令，关闭金山网镖 2008 的运行程序。



注　意　事　项

选择“操作”→“断开网路”命令后，“断开网路”命令会变成“恢复网络”命令。

技巧268　金山网镖 2008 的“工具”菜单

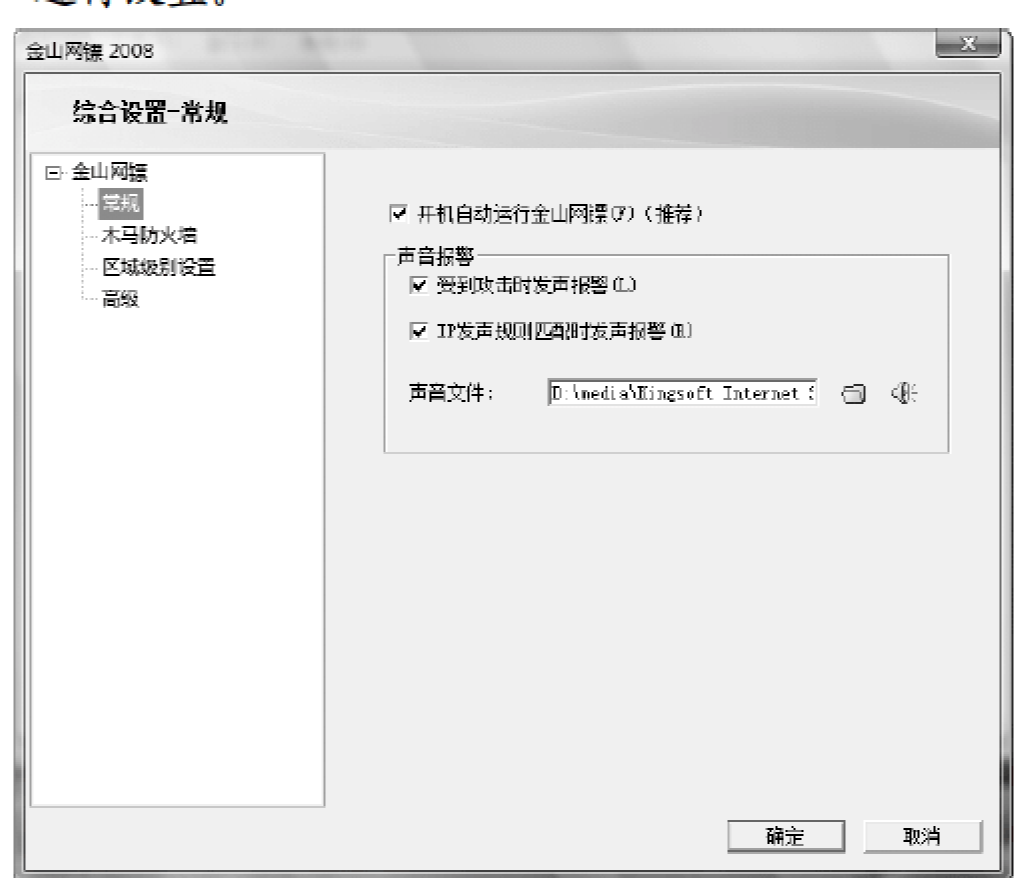
金山网镖 2008 的“工具”菜单下有“在线升级”、“日志查看器”和“综合设置”3 个功能。



- 选择“工具”→“在线升级”命令，弹出“金山毒霸在线升级程序”对话框，单击“下一步”按钮，即可进行升级，最后单击“完成”按钮。
- 选择“工具”→“日志查看器”命令，可以对金山网镖2008的日志记录进行查看和操作。



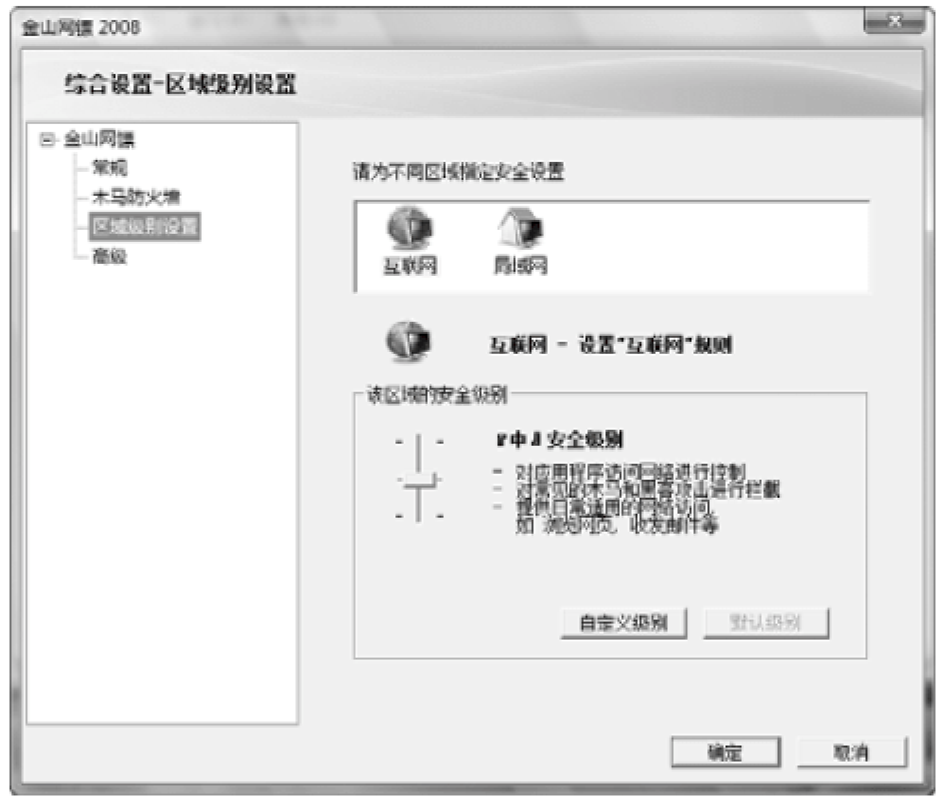
- 选择“工具”→“综合设置”命令可以对金山网镖2008进行设置。



注 意 事 项

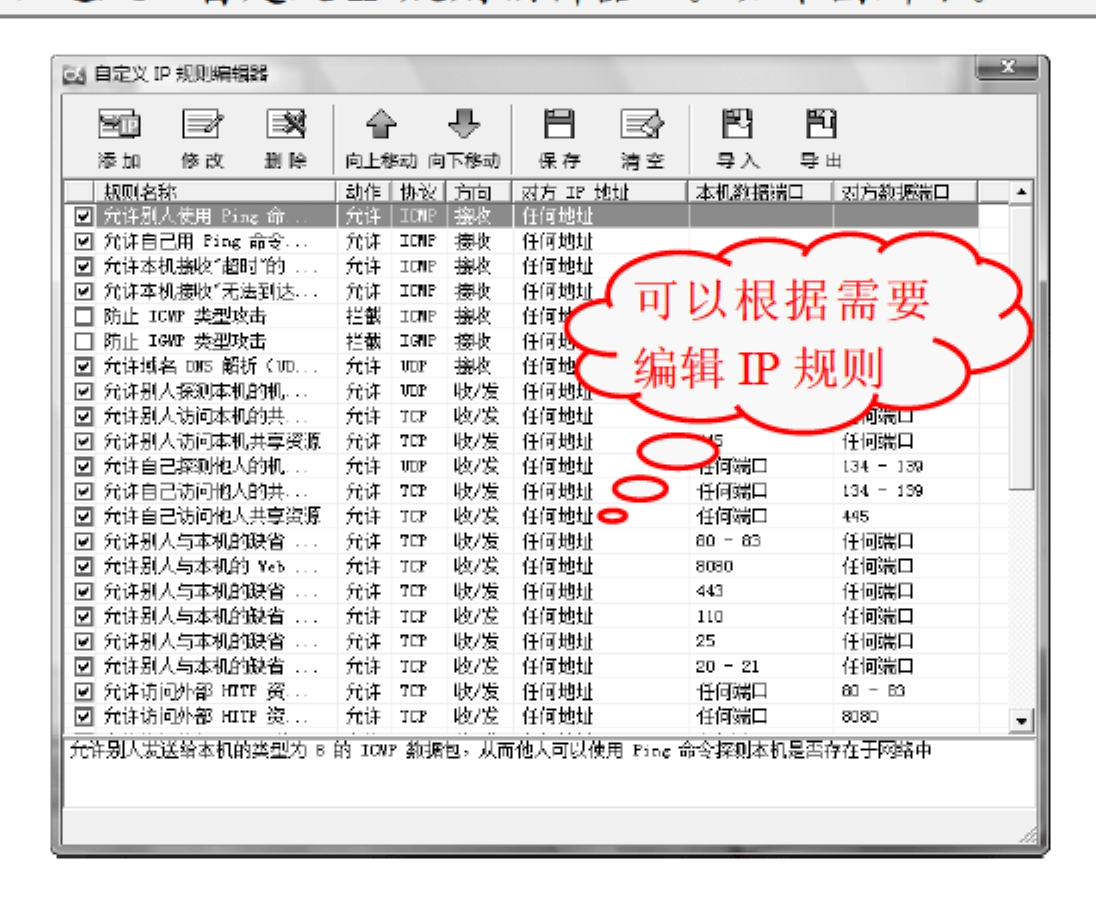
选中“开机自动运行金山网镖”复选框的功能和操作菜单下的“开机自动运行”命令是相同的效果。两种设置方法如下所示。





专 家 坐 堂

互联网区域设置互联网的安全级别，局域网区域设置局域网的安全级别，单击“自定义级别”按钮可以进入“自定义IP规则编辑器”。如下图所示。



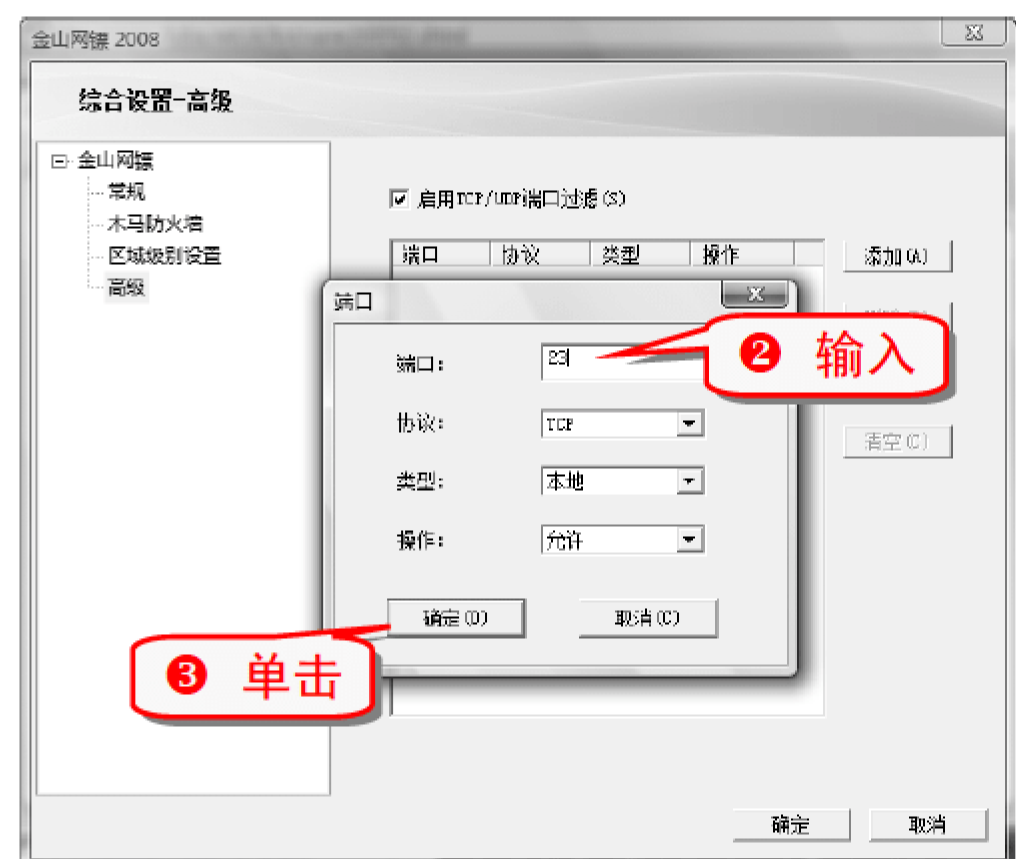
技巧269 手动添加IP包过滤规则，防范黑客攻击

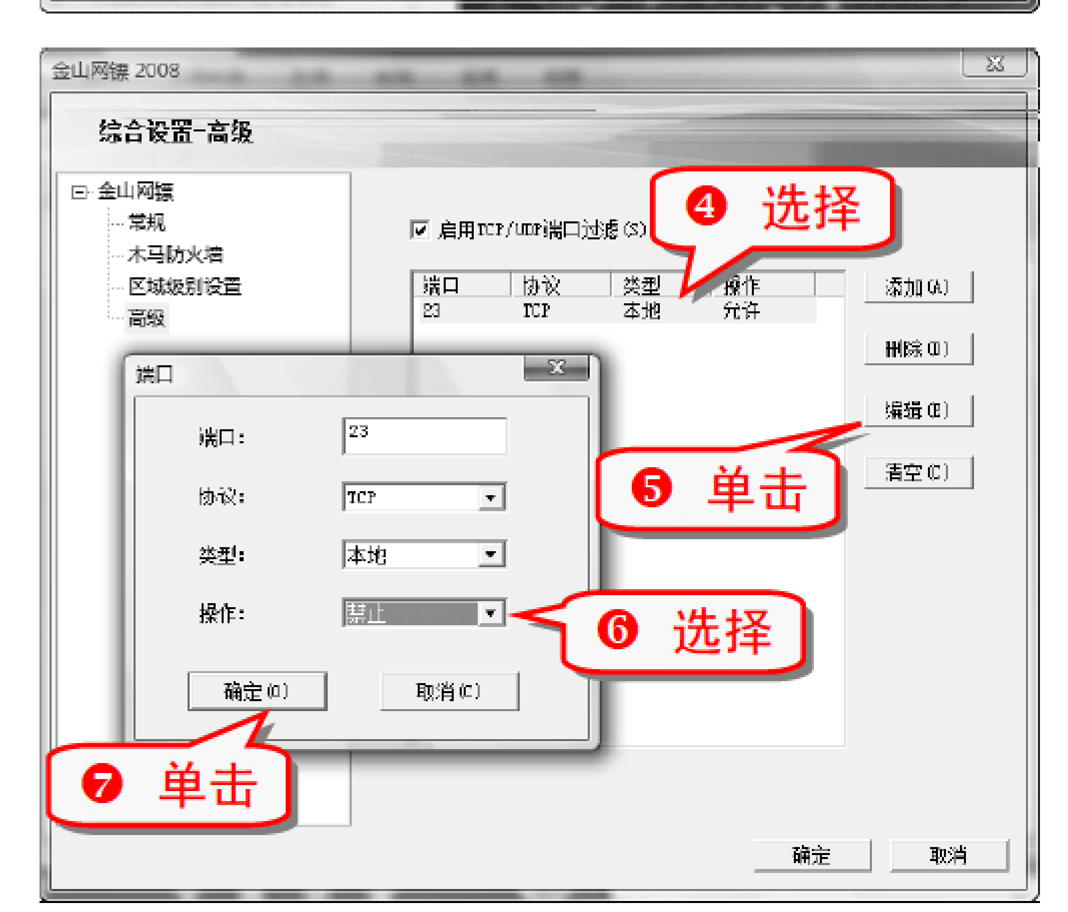
用户在金山网镖2008的“综合设置”窗口的“高级”页面中，可以使用IP包过滤技术，手动添加IP包过滤规



则，以达到防止黑客利用 IP 包和网络地址转换进行攻击的目的。









“添加”按钮：添加要过滤的端口。

“删除”按钮：删除不需要的过滤端口。

“编辑”按钮：对所选择的项进行编辑。

“清空”按钮：删除所有的过滤端口。

技巧270　金山网镖 2008 的“窗口”菜单

金山网镖 2008 的“窗口”菜单下有“安全状态”、“监控状态”、“应用规则”以及“网络状态”四项内容。



(1) 安全状态

“安全状态”选项卡包括“当前网络活动状态”和“网络活动日志”两部分。

“当前网络活动状态”选项组显示网络活动的详细状况，包括哪些程序已经连接网络以及网络发送和接收流量的情况。

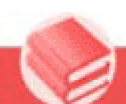
- 单击跳转到网络状态下，详细列出网络活动状态。
- 单击打开程序所在的目录。
- 单击结束所选择的程序。

“网络活动日志”选项组显示网络安全日志，可以及时发现网络威胁。

(2) 监控状态

“监控状态”选项卡显示互联网监控状态和局域网监控状态，在该选项卡中可以设置互联网和局域网的安全级别，还可以自定义 IP 规则。





知 识 补 充

上下滑动滑块选择不同的安全级别。

单击“默认设置”按钮恢复至默认级别。

单击“详细设置”按钮进入“自定义 IP 规则编辑器”界面。

(3) 应用规则

“应用规则”选项卡可以查看和更改应用规则权限的设置，对是否允许应用程序访问网络进行管理和操作。



(4) 网络状态

“网络状态”选项卡显示当前正在访问网络的程序和文件，并对其进行操作。



技巧271 瑞星个人防火墙 2008

瑞星个人防火墙 2008 具有完备的设置，有效监控网络连接，保护上网安全。其主界面上有四个按钮。



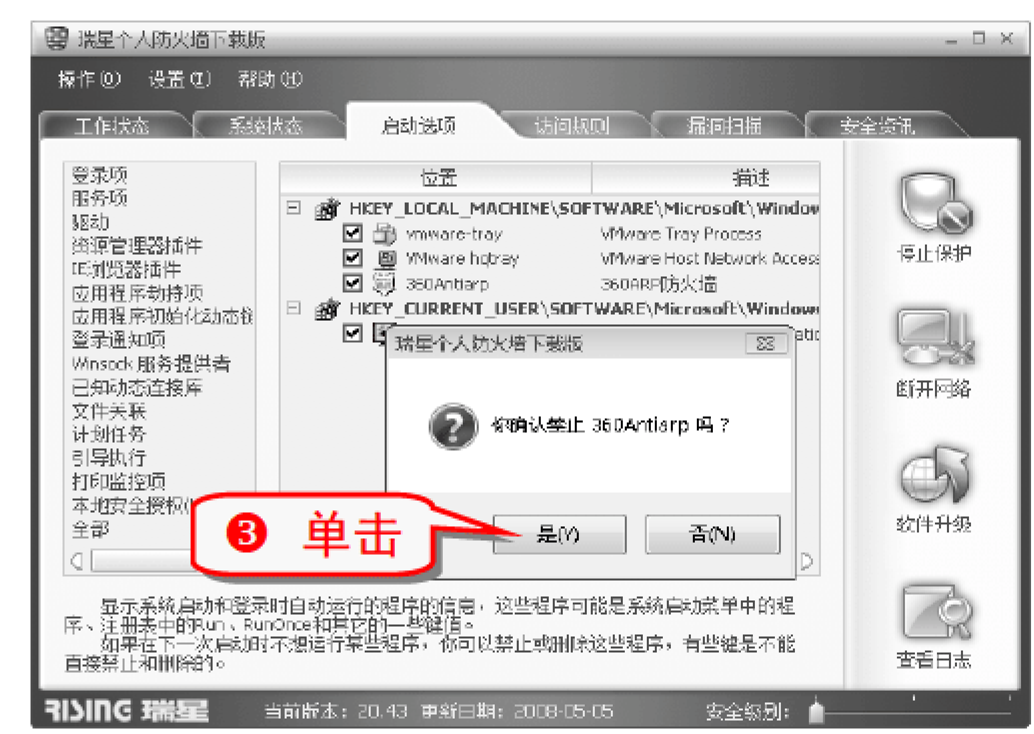
- 停止保护：停止防火墙的保护功能。
- 断开网络：将当前电脑与网络完全断开，无法从当前电脑访问网络，他人也无法从网络访问当前电脑。
- 软件升级：对防火墙进行升级更新。
- 查看日志：查看防火墙的所有日志。

技巧272 瑞星个人防火墙 2008 的启动选项

在瑞星个人防火墙 2008 的“启动选项”选项卡中可以禁用不需要在开机时运行的程序。

❶ 在瑞星个人防火墙 2008 主界面上切换到“启动选项”选项卡。



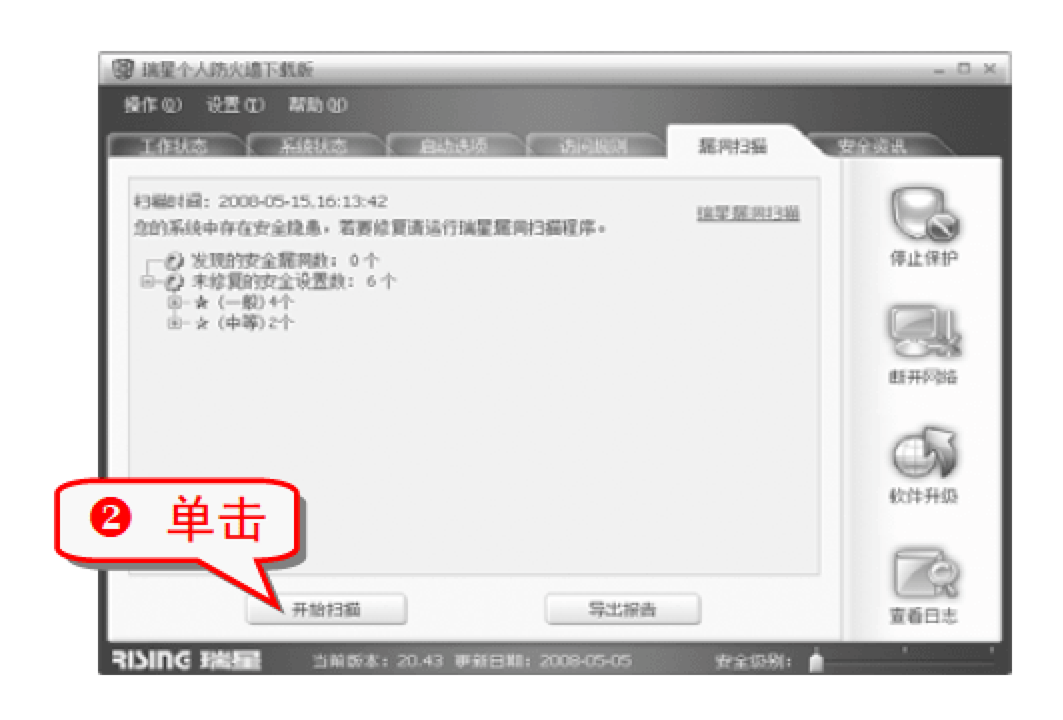


技巧273 使用瑞星个人防火墙 2008 扫描漏洞

漏洞扫描是指扫描系统中存在的安全隐患，并对其进行修复。

❶ 在瑞星个人防火墙 2008 主界面上切换到“漏洞扫描”选项卡。





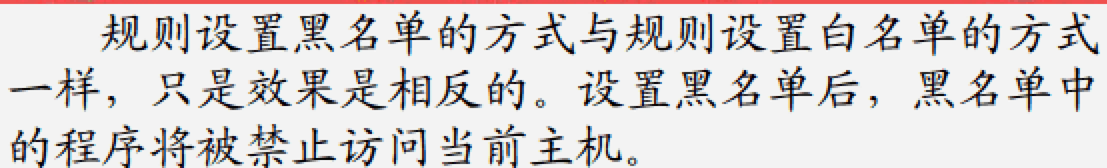
技巧274　使用瑞星个人防火墙 2008 规则设置白名单

瑞星防火墙和其他应用软件一样，凡是涉及控制方面几乎都应用了黑白名单规则，简单地说，白名单就是允许通过的用户、IP、软件或数据流，设置的名单可以对允许通过的用户 IP 软件和数据流等进行更好地筛选。

❶ 在瑞星个人防火墙 2008 主界面上选择“设置”→“详细设置”命令。







规则设置黑名单的方式与规则设置白名单的方式一样，只是效果是相反的。设置黑名单后，黑名单中的程序将被禁止访问当前主机。

技巧275　傲盾 DDOS 防火墙

傲盾 DDOS 防火墙是一款针对各种网站、信息平台、Internet 服务等，集多种功能为一体的安全平台，能够检测网络协议中所有层的状态，有效阻止 DOS、DDOS 等各种攻击。



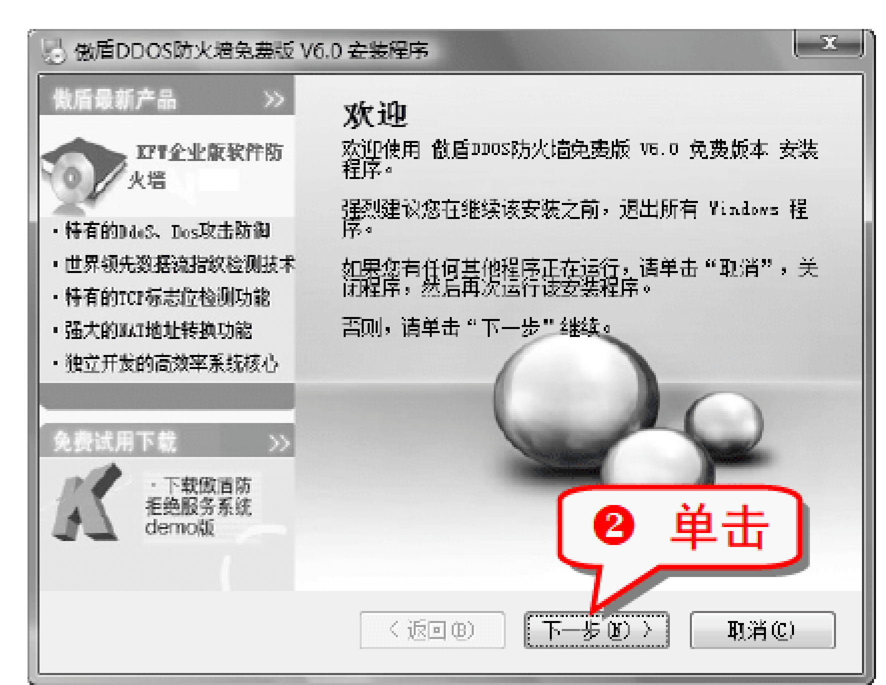
专 家 坐 堂

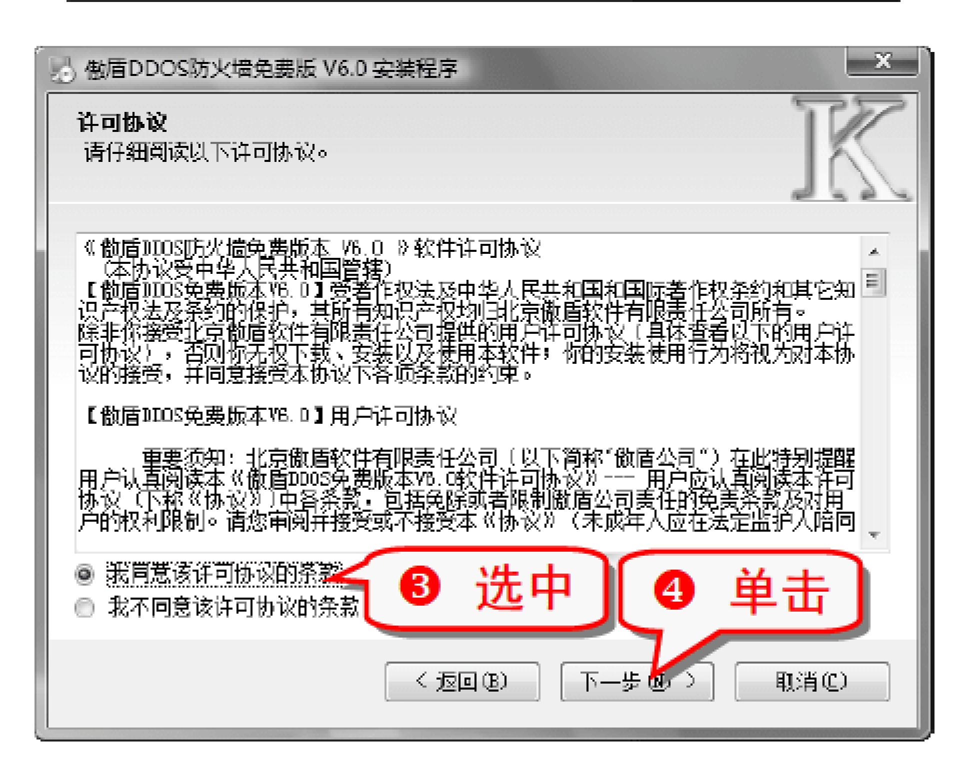
傲盾 DDOS 防火墙具有以下功能。

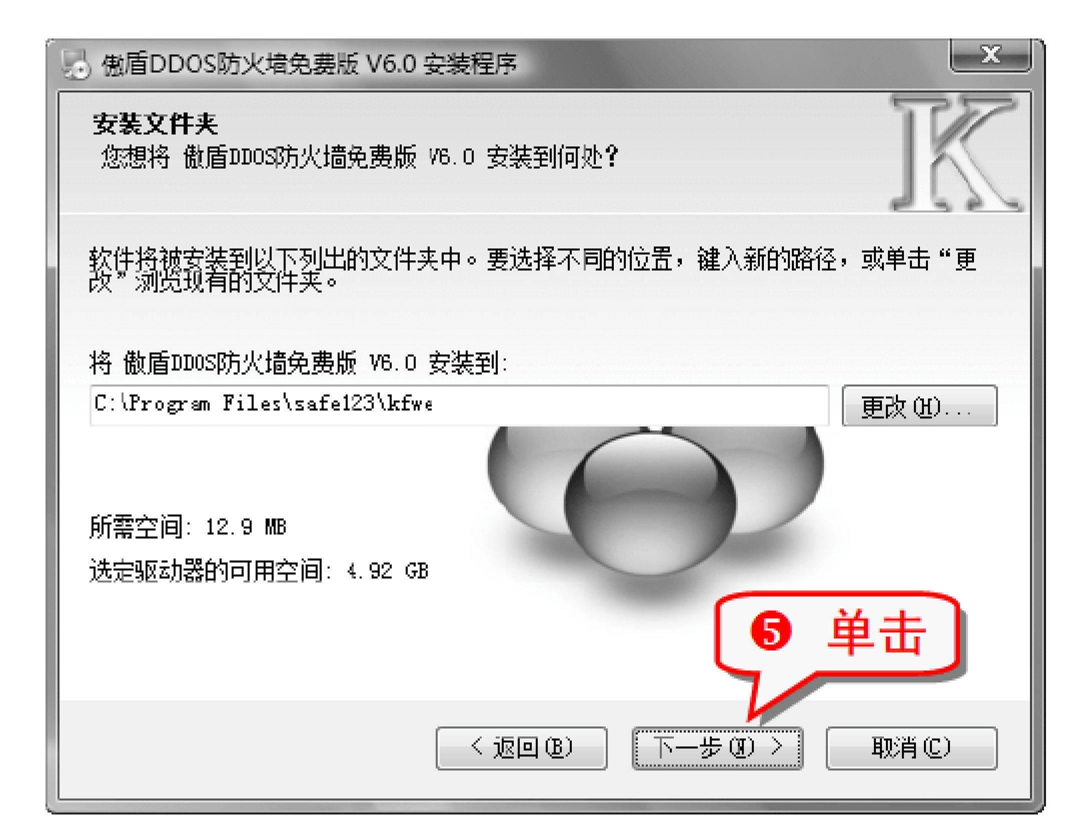
- 数据包规则过滤。
- 数据流指纹检测过滤。
- 数据包内容定制过滤。
- NAT 功能(支持 FTP PASV 和 port，支持 irc 的 ddc 等动态端口模式，安装防火墙后不用设置 PASV 之类的端口)。
- 端口映射功能。
- 流量控制。
- 强大的包抓分析模块。
- log 模块。
- 采用最先进的数据流指纹技术，提供强大的 DOS(拒绝服务)攻击防护，彻底防护各种已知和未知的 DOS 攻击。
- 流量分析监测。
- 实时访问连接监控。
- 支持 DMZ 区的建立。
- 账号，权限管理。
- 分布式管理。

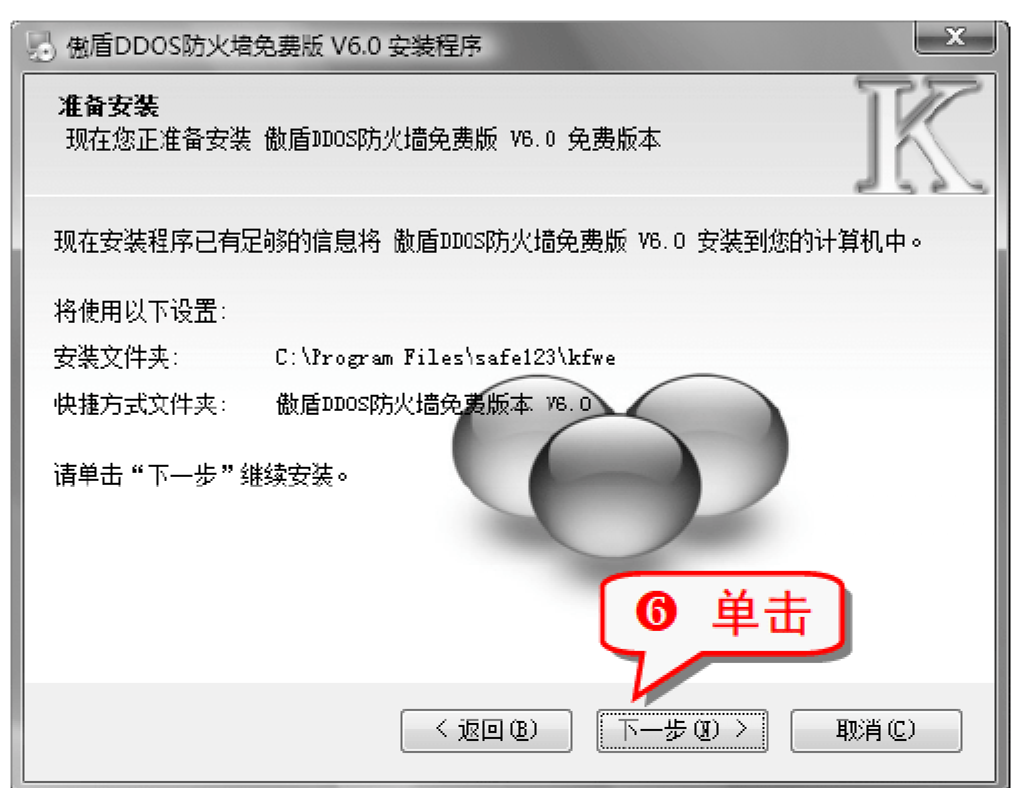
技巧276　快速安装傲盾 DDOS 防火墙

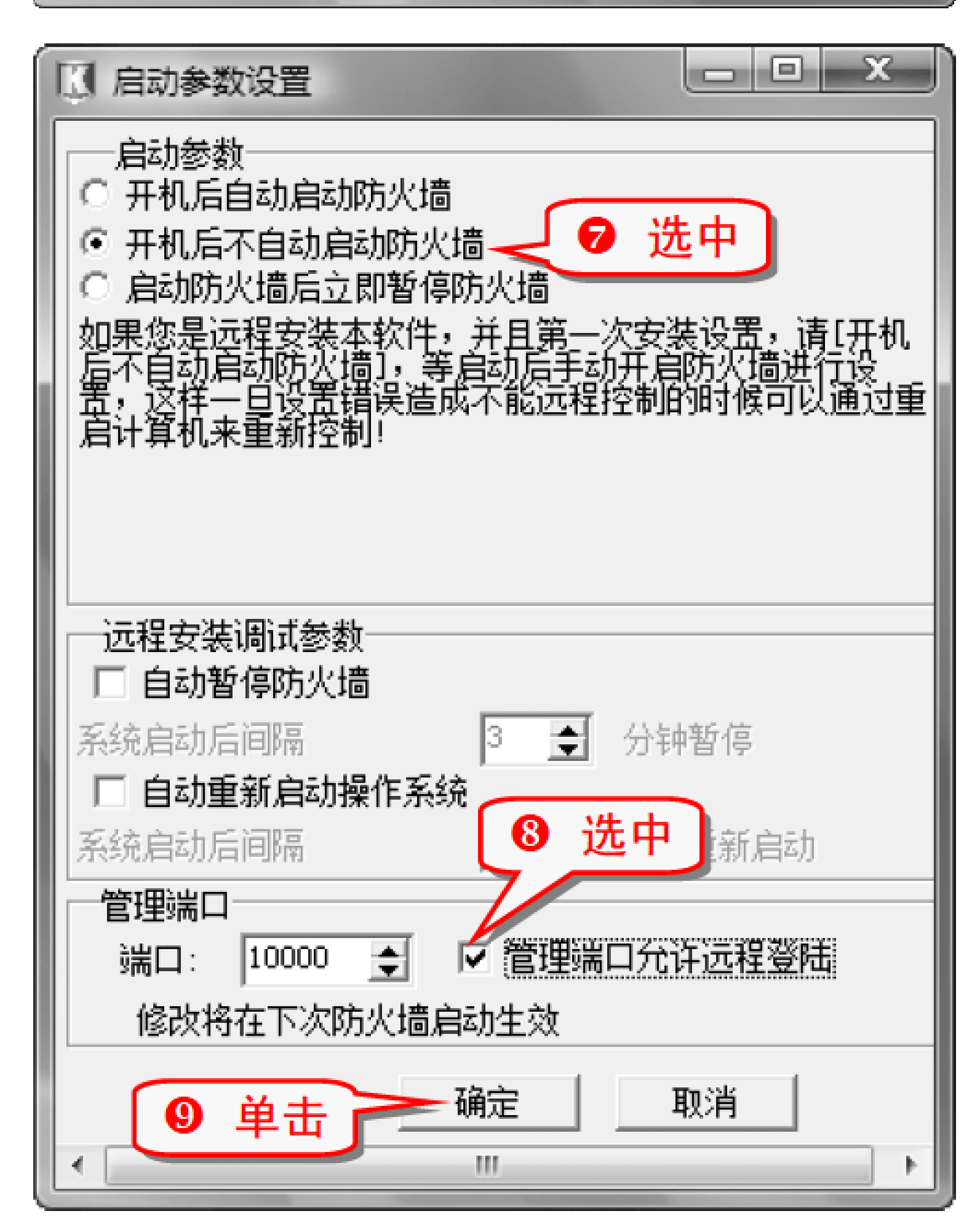
❶ 下载安装包后双击打开安装程序。

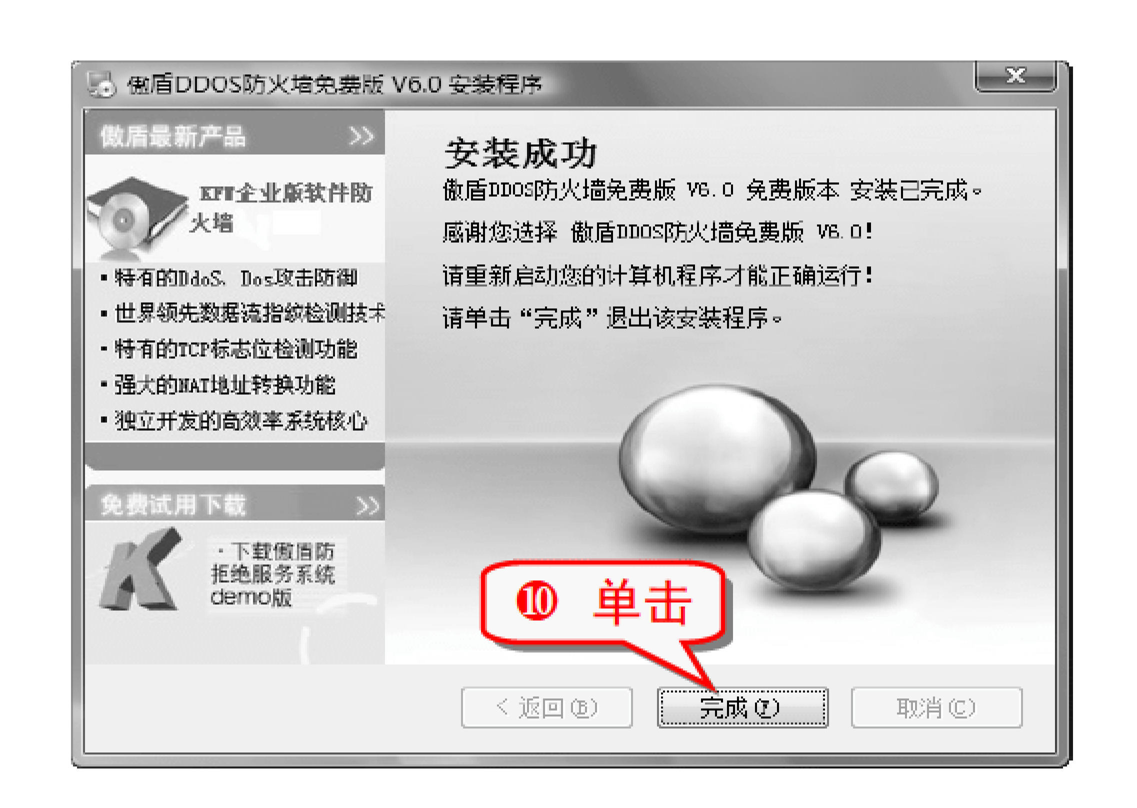












技巧277 调试傲盾 DDOS 防火墙

❶ 完成防火墙的安装，重新启动电脑，选择"开始"→"所有程序"→"傲盾防火墙免费版本 V6.0"→"运行托盘"命令。

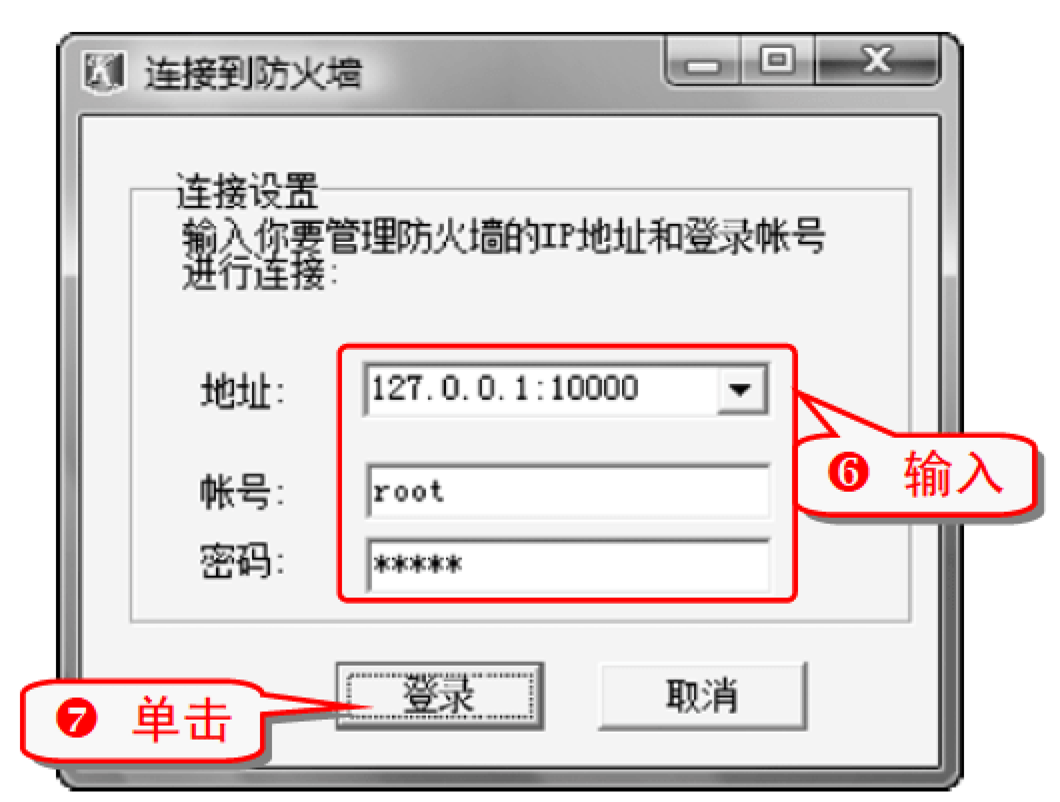
❷ 运行托盘后，在桌面右下角任务栏会出现下图所示的傲盾小图标。



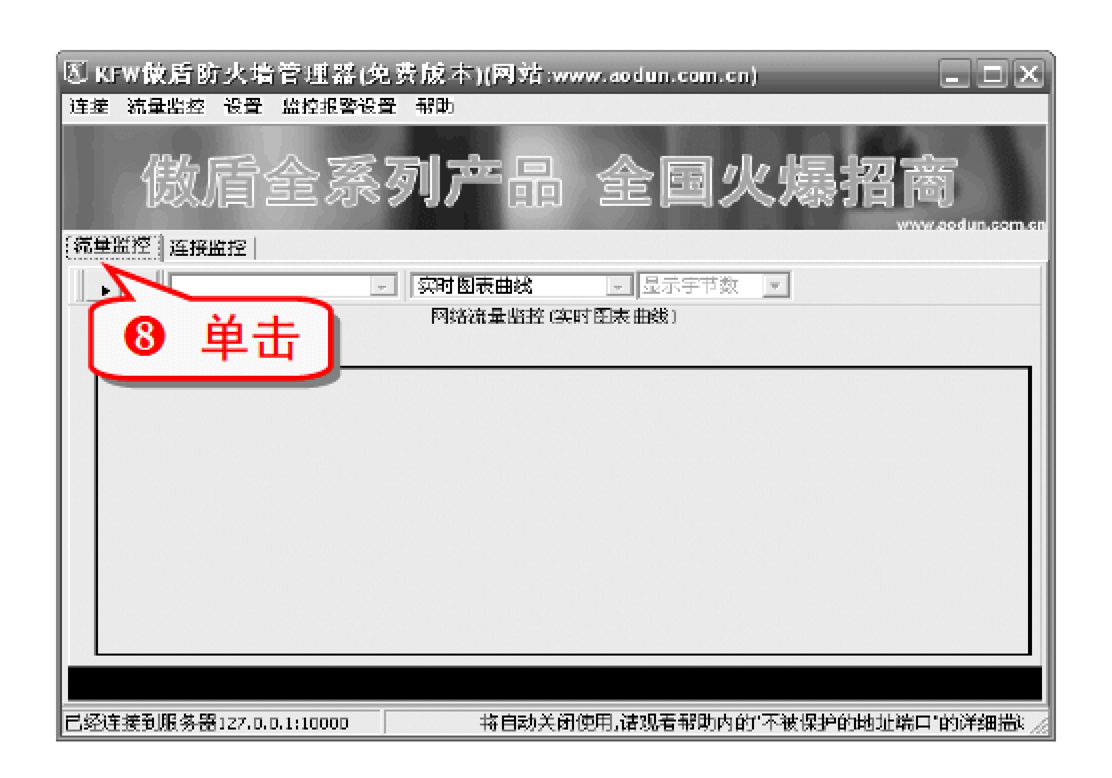
❸ 双击此图标，出现下图所示的页面。

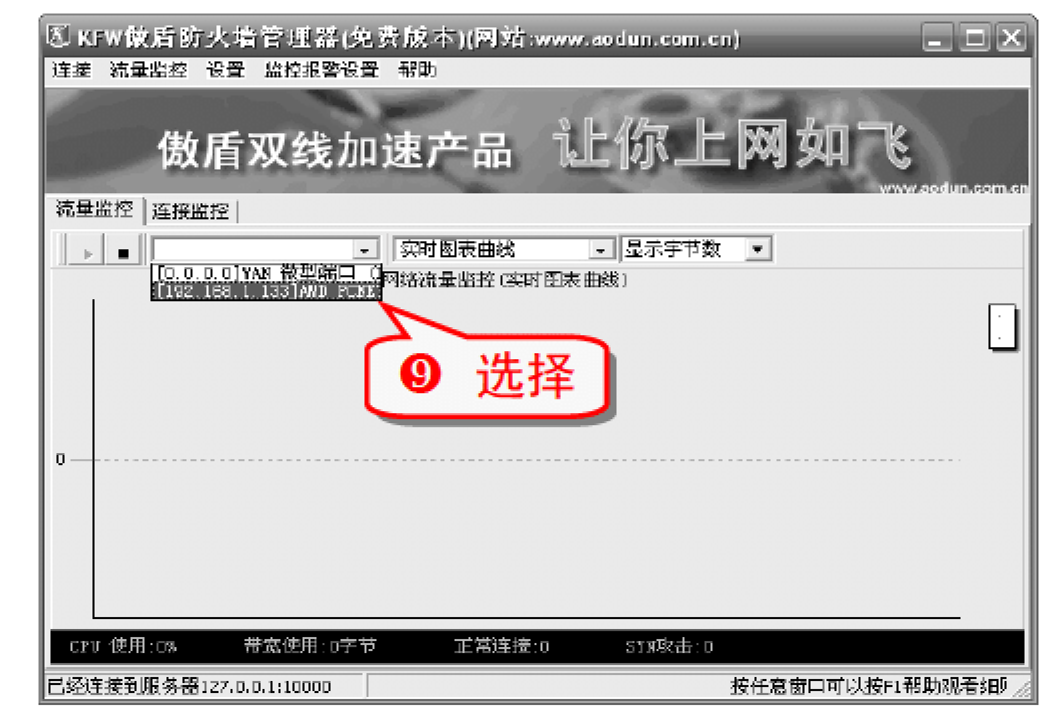


❺ 双击桌面上的"KFW 企业管理器"图标，弹出防火墙管理器登录界面。

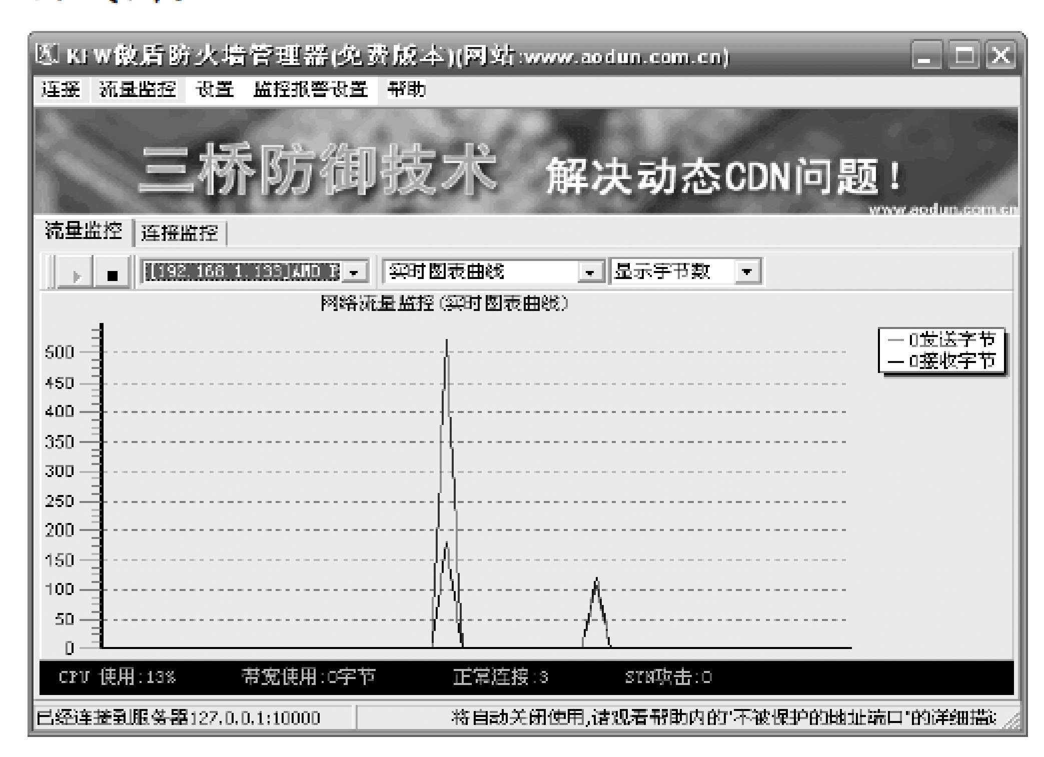






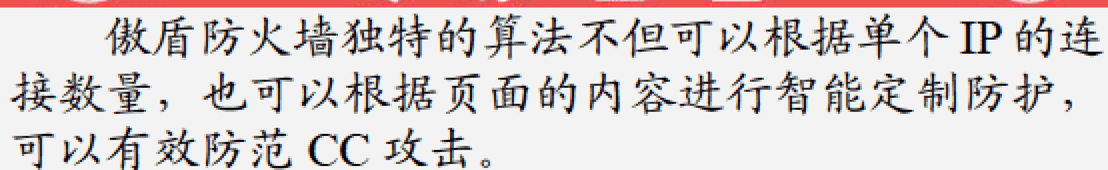


❿ 选中防火墙绑定的 IP 后，会出现流量监控的实时图表曲线图。



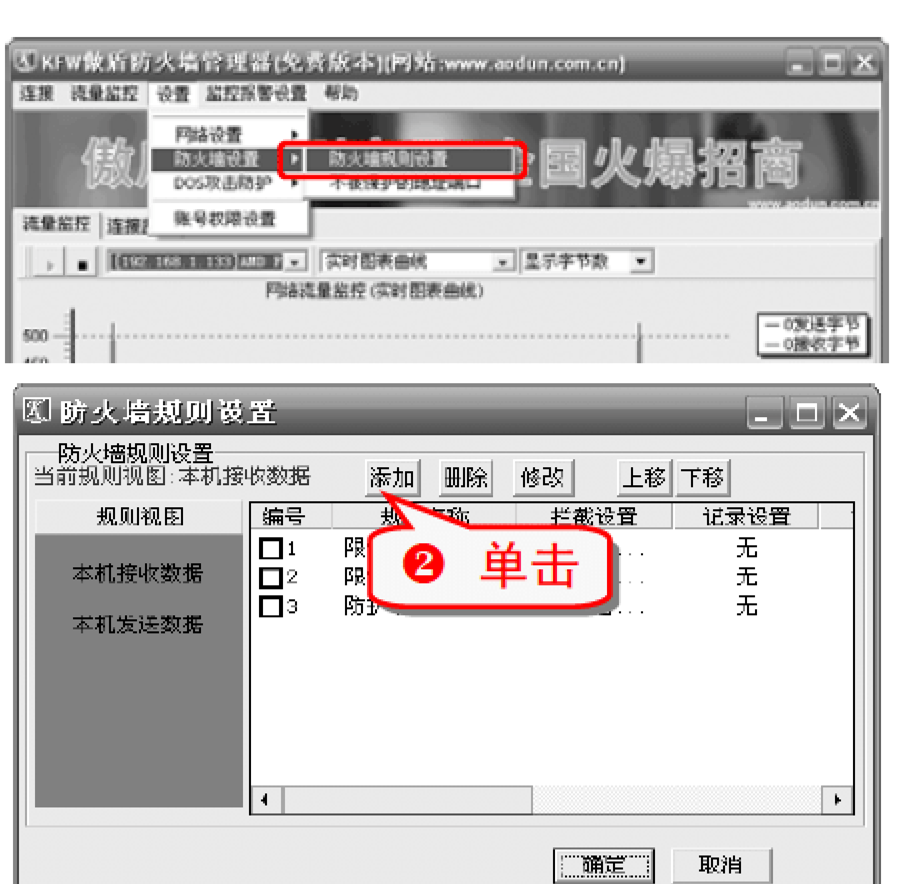
技巧278　使用傲盾 DDOS 防火墙防范 CC 攻击

CC 攻击是 DDOS 攻击的一种，CC 攻击是模拟多个用户不停地进行访问某个页面直至系统崩溃。

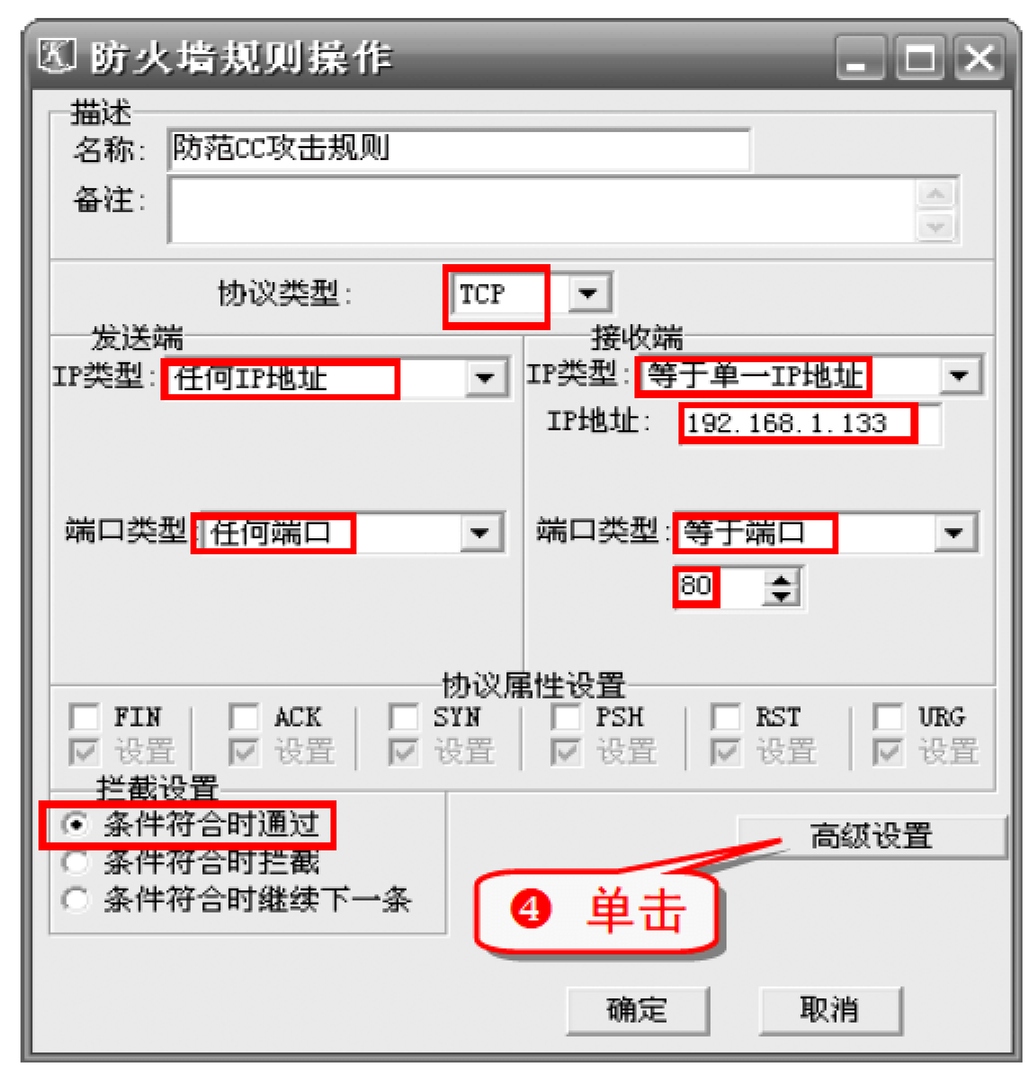


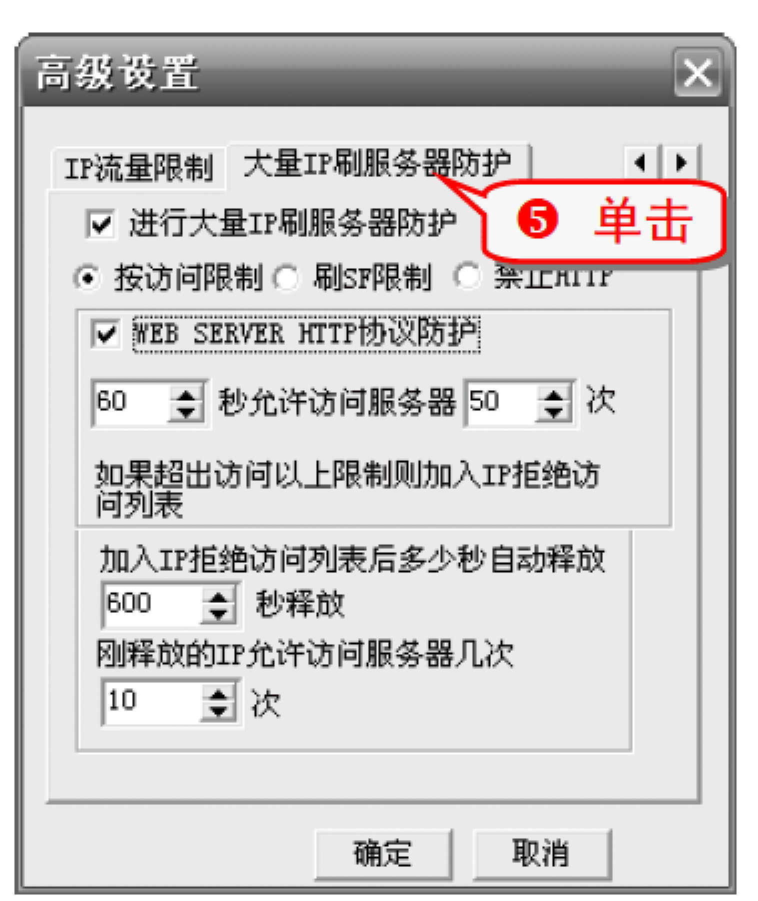
傲盾防火墙独特的算法不但可以根据单个 IP 的连接数量，也可以根据页面的内容进行智能定制防护，可以有效防范 CC 攻击。

❶ 打开“KFW 傲盾防火墙管理器”，选择“设置”→“防火墙规则”→“防火墙规则设置”命令。



❸ 在“名称”文本框中输入“防范 CC 攻击规则”，协议类型选择 TCP，发送端的 IP 类型选择“任何 IP 地址”，端口类型选择“任何端口”，接受端的 IP 类型选择“等于单一 IP 地址”，并输入当前电脑的 IP 地址，端口类型选择“等于端口”数字为 80(通常 Web 服务器的端口是 80)。拦截设置下选中“条件符合时通过”。





❻ 按上图所示进行设置以后单击“确定”按钮，完成防范 CC 攻击的设置。

技巧279　江民防火墙

江民防火墙是一款为解决个人用户上网安全而设计的网络安全防护工具，可以防范黑客攻击、木马程序及互联网病毒等各种网络危险的入侵，全面保护个人上网安全。

安装完江民防火墙后会在通知区域出现一个盾牌图标。



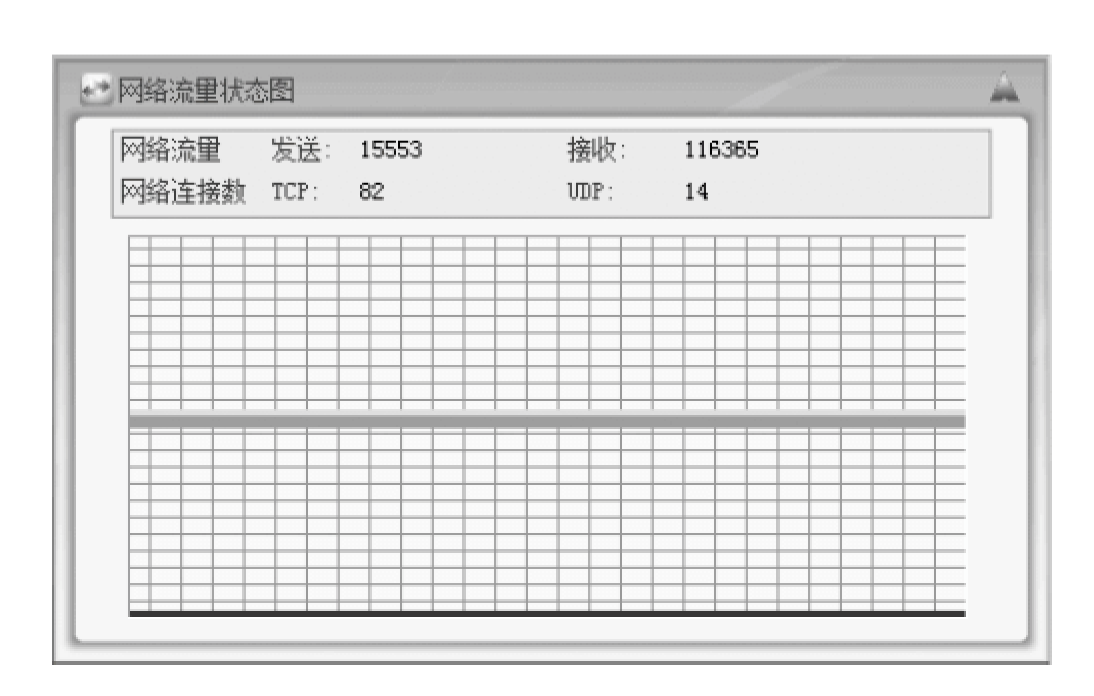
双击图标即可打开江民防火墙的主菜单。



技巧280　剖析江民防火墙的系统信息

在系统信息页面中记录着当前防火墙的一些数据统计和运行状态。

单击防火墙主菜单上的“网络流量状态”就能弹出“网络流量状态图”。



“发送”后面的数据代表当前整个系统发送至网络的数据流量统计。

“接收”后面的数据代表当前整个系统接收来自网络的数据流量统计。

TCP 后面的数据代表当前系统打开 TCP 协议连接的数量。

UDP 后面的数据代表当前系统打开 UDP 协议连接的数量。

单击“当前网络连接”即可弹出“当前网络连接”界面，列出当前系统中的所有连接状态。






知　识　补　充

IP：该连接的 IP 地址。

TCP：该连接的连接和侦听地址及端口。

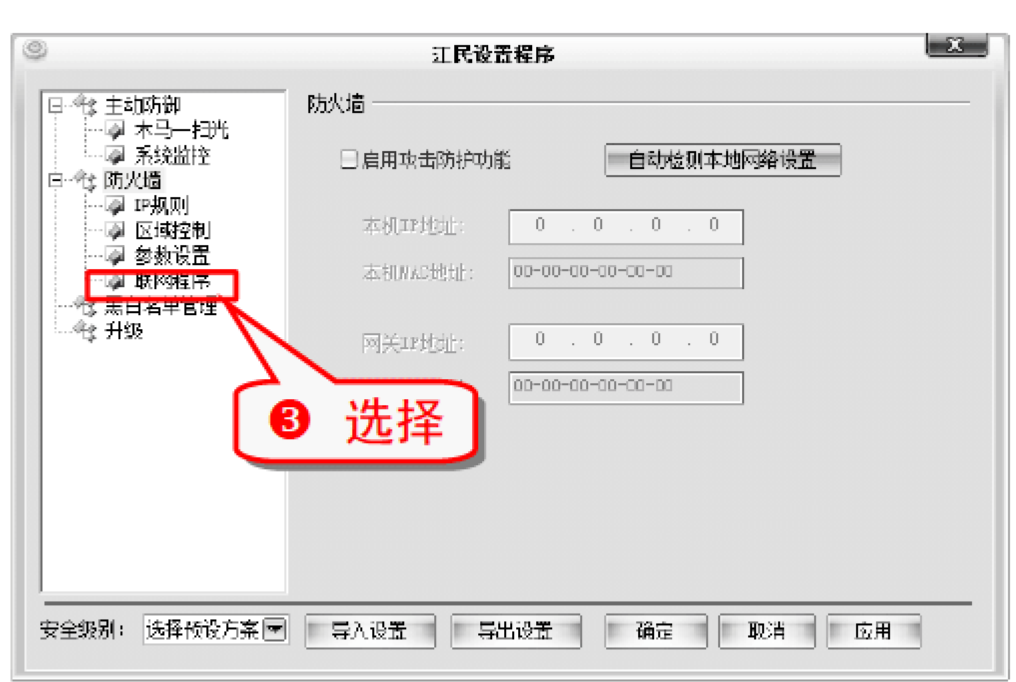
UDP：该连接的 UDP 地址及端口。

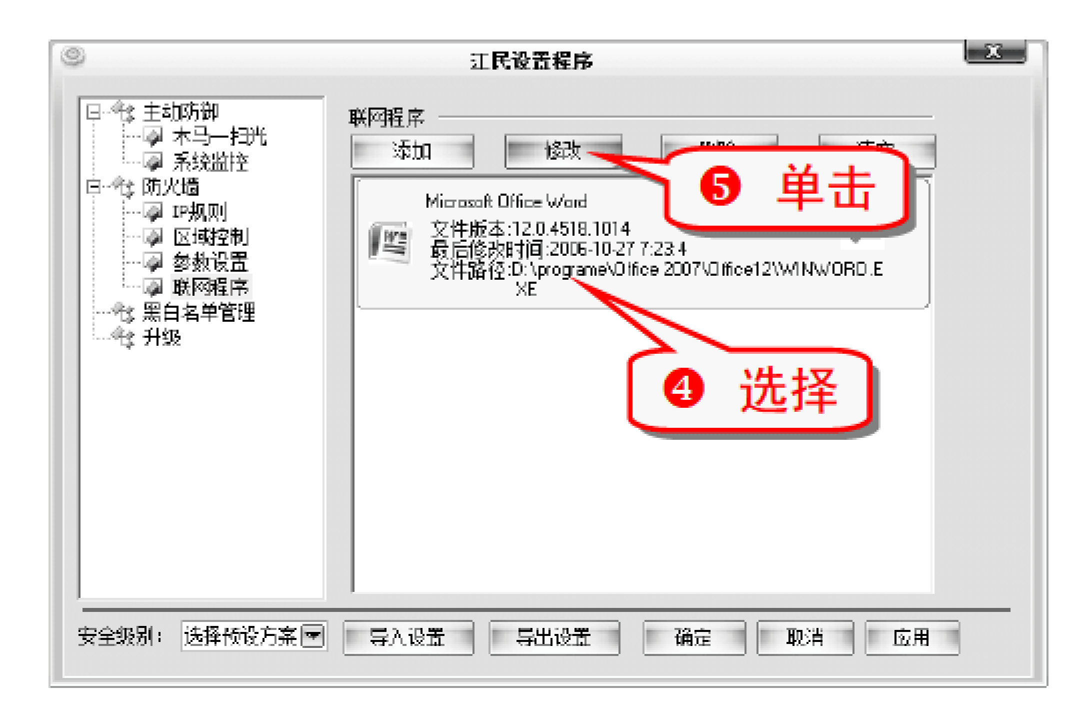
技巧281　设置江民防火墙应用程序审核

在设置管理中，选择防火墙在下拉菜单下单击“联网程序”选项，可以查看到当前认证过的应用程序，可以对其进行重新审核。

❶ 打开江民防火墙。









❻ 当单击“修改”按钮后出现如下窗口，这里可以选择如何审核程序。



技巧282　智能升级江民防火墙

江民防火墙的智能升级功能主要是对防火墙版本及相关模块的升级。









技巧283　设置江民防火墙的活动日志

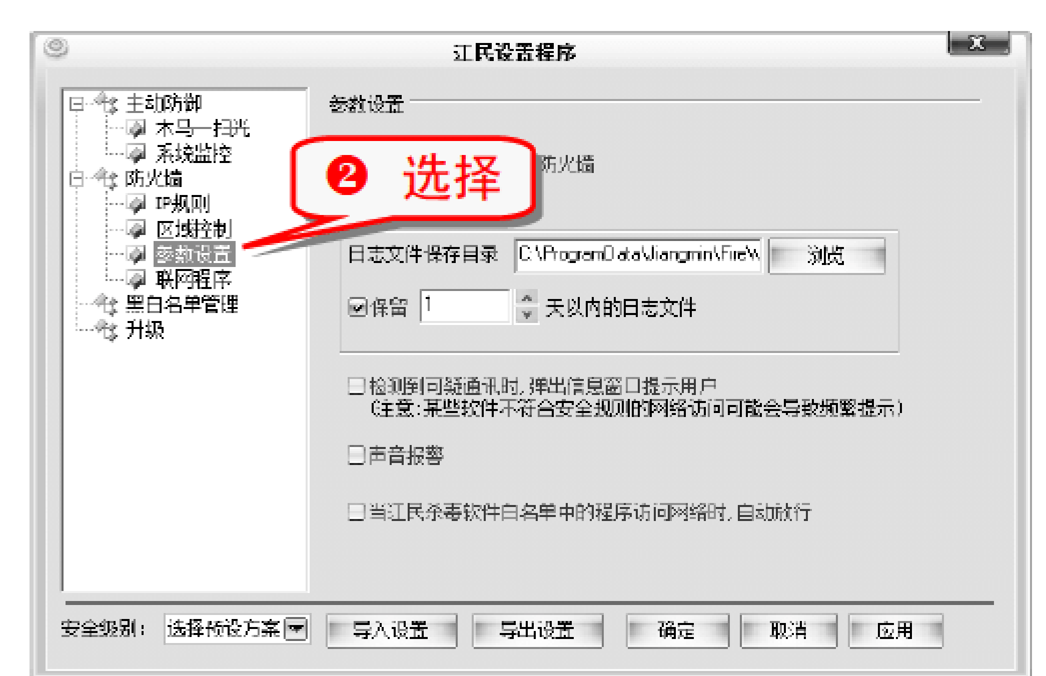
江民防火墙的网络活动日志中包含的内容有：记录的具体时间、应用程序、本地地址、远程地址以及处理的方式等。

单击防火墙主菜单上 网络活动日志 就能弹出“网络活动日志”界面。



对日志进行设置的步骤如下。

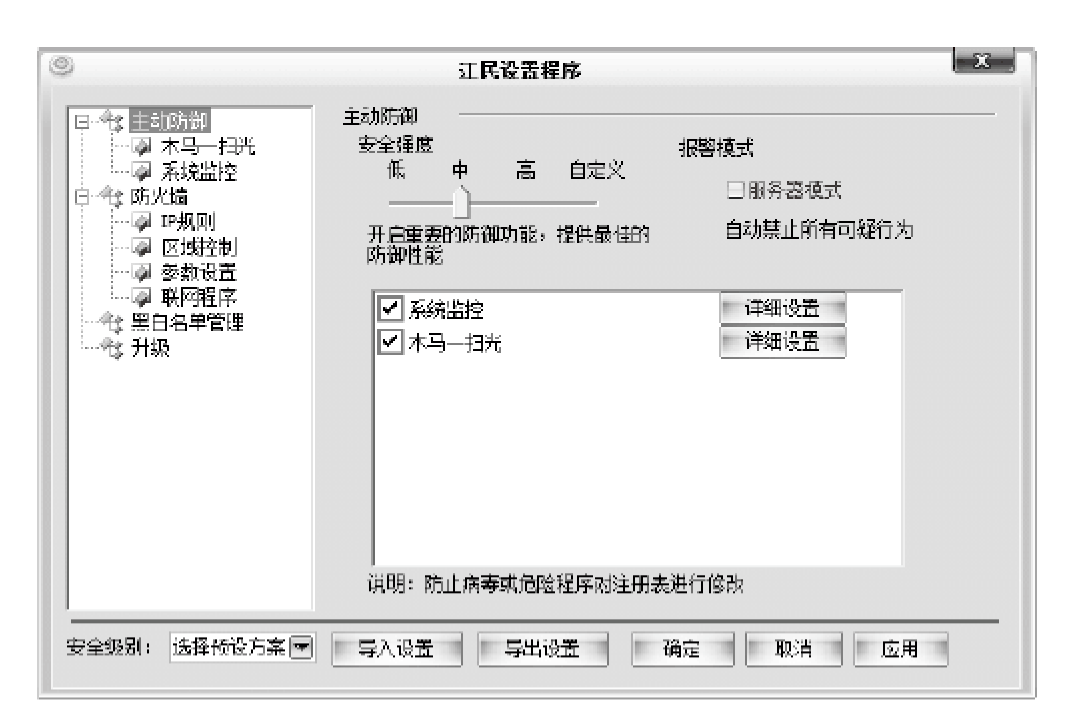




❸ 接下来就可以在该界面中对日志进行设置。

技巧284　设置江民防火墙主动防御模块

主动防御模块包括木马一扫光和系统监控。



专 家 坐 堂

“系统监控”是一个在后台运行功能强大的组件，可以根据在系统中运行进程的部分特征，比如是否在系统文件夹中创建了文件、是否是注入进程、是否向外部发送了邮件和是否访问过物理内存等来自动智能判断当前在系统中运行的进程是否存在病毒或木马程序。

木马一扫光：“木马一扫光”是防止木马程序入侵用户电脑的专业监控程序，在运行木马一扫光监控后，一旦发现木马或类似木马的不明程序在用户的电脑中修改注册表、记录键盘以及鼠标操作时，木马一扫光就会及时向用户报警，提醒用户进行相应的操作。

技巧285 龙盾 IIS 防火墙

龙盾 IIS 防火墙是一款专门针对 IIS 的安全防护软件，具有以下功能。

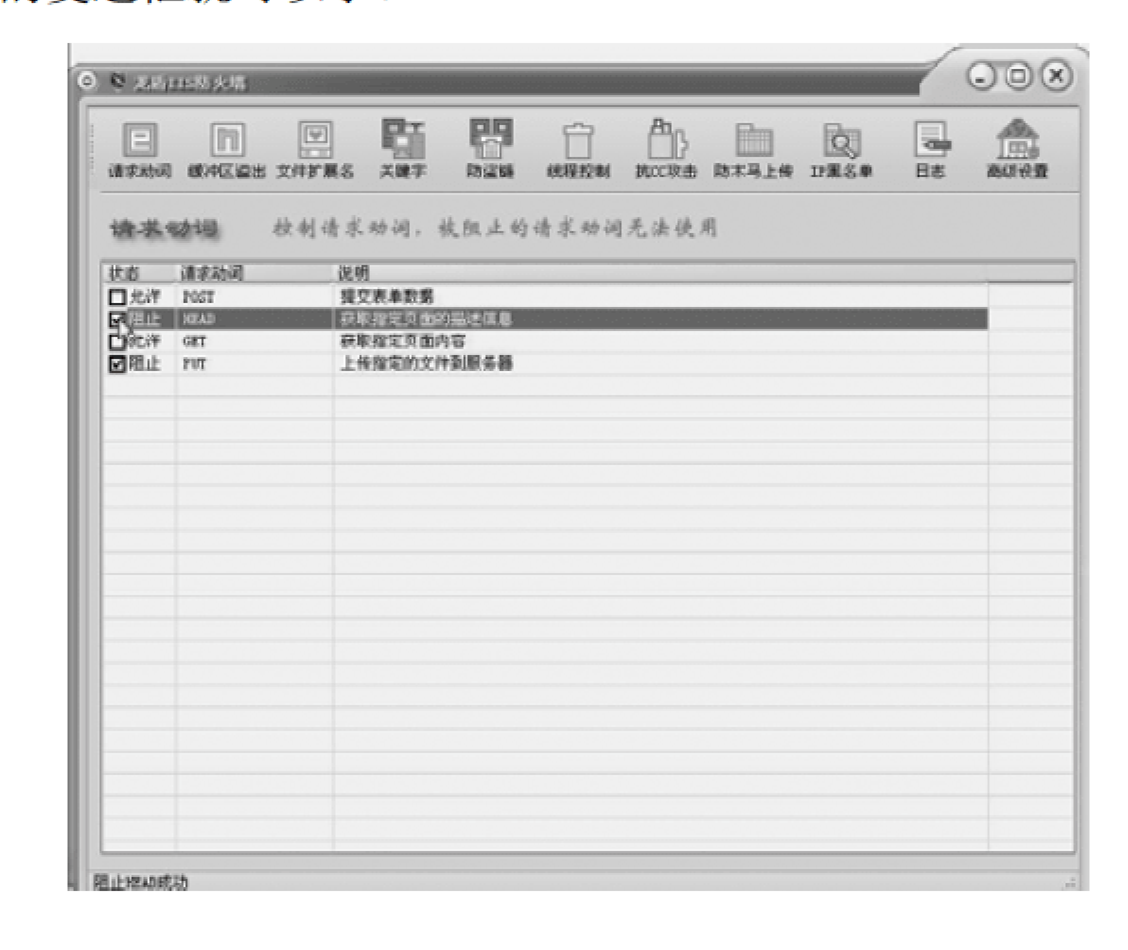
- 专业 SQ 注入：不仅可以过滤普通关键字，而且支持“模式匹配”功能。
- 实用防盗链：只需要简单设置，即可保证网站资源不被其他网站盗链。
- 线程控制：随意控制文件下载的线程数量以及下载速度。
- 抗 CC 攻击：有效抵御 CC 和 DDOS 软件的攻击。
- 禁用代理：根据需要，可启用或禁用代理服务器的访问。
- IP 地址黑名单：任意阻止某 IP 地址的访问。
- 抗缓冲区溢出攻击：可自定义 URL 地址长度以及 HTTP 长度。
- 防止源代码泄露：有效禁止非法脚本执行，防止源代码泄漏。
- 防止木马上传：防止通过 HTTP 方式上传病毒和木马程序。
- 禁止下载：可根据需要，只允许在线播放音频或视频。

技巧286 设置龙盾 IIS 防火墙请求动词

在 HTTP 协议中，请求动词表示用户以何种方式访问网站，主要动词有 GET、POST 和 HEAD 等。

(1) 改变动词的访问状态

要改变某个请求动词的状态，只要单击选择状态栏中的复选框就可以了。

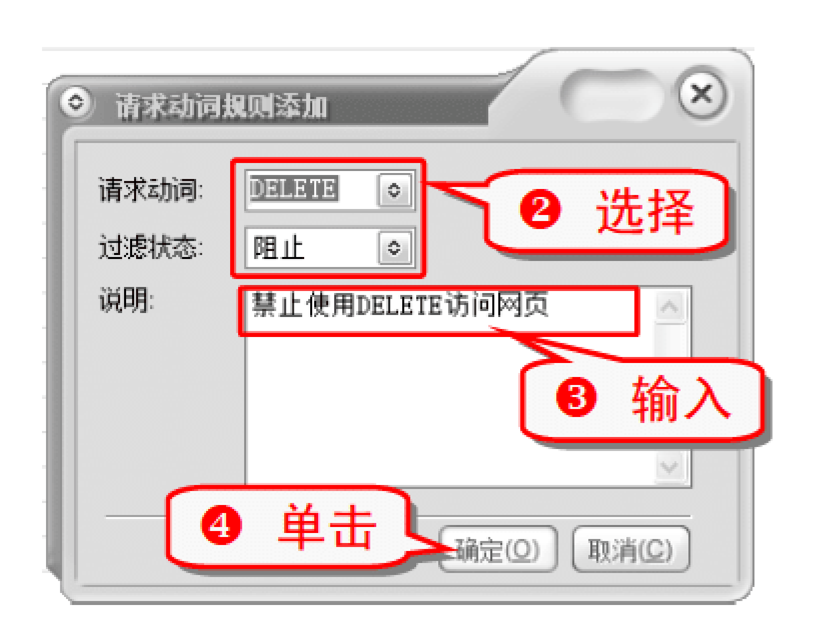


(2) 添加访问动词规则

❶ 右击空白处，在弹出的快捷菜单中选择“添加”命令。



在随后的添加规则对话框中添加指定的规则。例如添加一个 DELETE 动词规则。



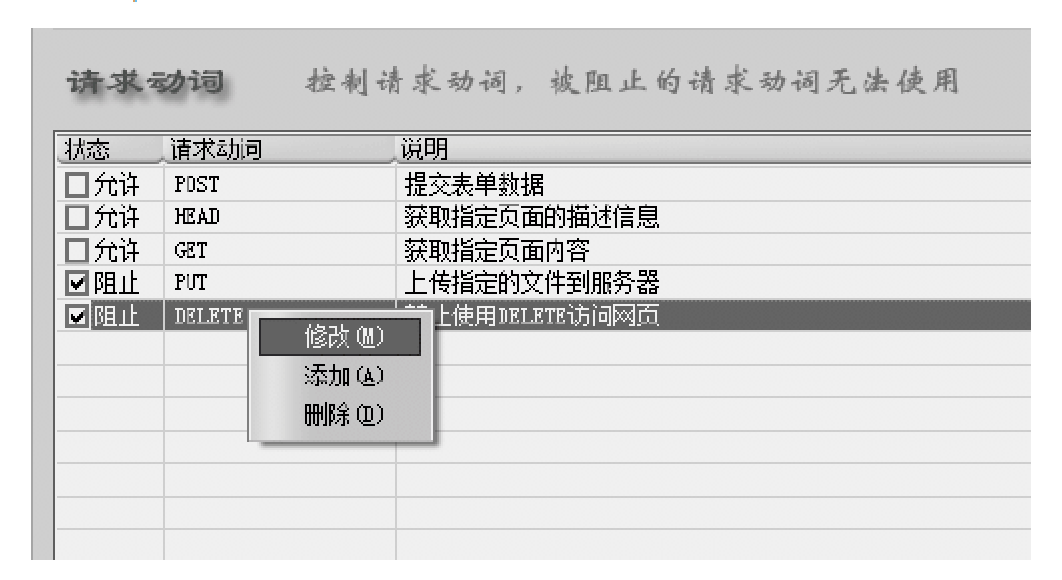
状态	请求动词	说明
☐允许	POST	提交表单数据
☐允许	HEAD	获取指定页面的描述信息
☐允许	GET	获取指定页面内容
☑阻止	PUT	上传指定的文件到服务器
☑阻止	DELETE	禁止使用DELETE访问网页



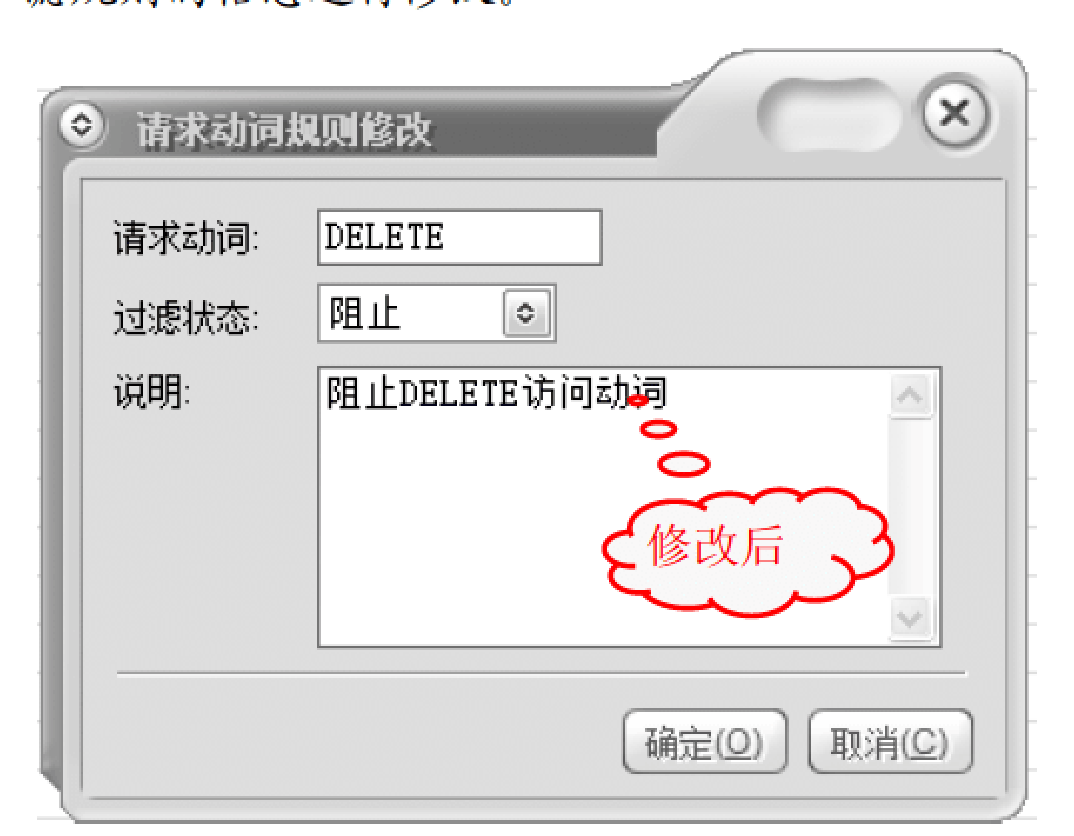
如果有用户通过动词 DELETE 访问网站，龙盾 IIS 防火墙会拦截用户的访问。

(3) 修改访问动词规则

❶ 右击选中的过滤规则，在弹出的快捷菜单中选择“修改”命令。



❷ 在弹出的“请求动词规则修改”对话框中，对当前过滤规则的信息进行修改。



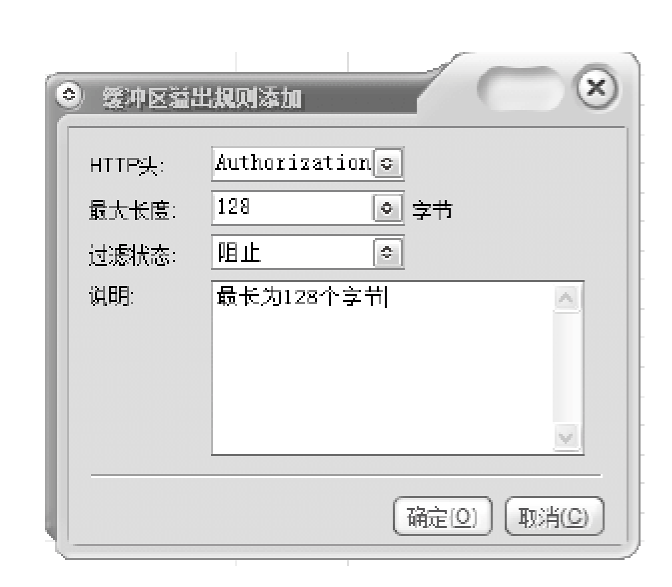
技巧287　添加龙盾 IIS 防火墙缓冲区溢出规则

由于 Web 服务器本身的缺陷和漏洞，当用户提交超大容量的数据时，可能会导致 Web 服务器崩溃或者被黑客截获。众所周知的“红色代码”和“Nimda 蠕虫”病毒就是利用缓冲区溢出规则发动攻击的。利用龙盾 IIS 防火墙可以限制用户提交的数据长度。

缓冲区溢出　控制HTTP请求头长度，超过指定长度，请求被禁止

状态	HTTP头域	最大长度	说明
☑阻止	Accept:	1024	接收数据的类型
☑阻止	Referer:	2048	包含一个URL，从这个URL访问当前请求页面
☑阻止	Cookie:	2048	保存在客户端的关于web的状态信息
☑阻止	Host:	1024	请求页面所在地

❶ 右击空白处，在弹出的快捷菜单中选择“添加”命令，在弹出“缓冲区溢出规则添加”对话框中添加指定的规则，例如要添加溢出规则 Authorization:，其最大数据量为 128 个字节，并将其状态置为“阻止”。



❷ 单击“确定”按钮后，溢出规则 Authorization:就被添加到过滤规则列表内了，如果有用户向网站发送带有 Authorization:头域的数据包，其值超过了 128 个字节，龙盾 IIS 防火墙会拦截此数据包。

技巧288　使用龙盾 IIS 防火墙阻止访问指定类型文件

利用龙盾 IIS 防火墙可以阻止用户访问指定类型的文件，从而保证网站和数据的安全。



在软件主窗口中可以进行“改变文件扩展名规则的状态”、“添加文件扩展名规则”、“修改文件扩展名规则”以及“删除文件扩展名规则”等操作。操作方法跟“请求动词”部分的操作大致相同。

技巧289　为龙盾 IIS 防火墙添加 SQL 注入过滤规则

龙盾 IIS 防火墙采用先进的系统接口，结合“模式匹配”技术，可对用户提交的 Web 数据进行全面的分析和过滤，从而有效地阻止 SQL 注入，保证网站的安全。




知 识 补 充


SQL 注入是指：攻击者通过发送精心构造的 SQL 数据包，绕过网站和数据库的验证机制，取得后台的控制权，获取账号和密码等敏感信息。

对于关键字的操作包括以下四种。

- 改变 SQL 注入(关键字)过滤规则。
- 添加 SQL 注入(关键字)过滤规则。
- 修改 SQL 注入(关键字)过滤规则。
- 删除 SQL 注入(关键字)过滤规则。

例如，要添加 SQL 注入过滤规则 sum(，并将其状态设置为“阻止”，则设置方法如下图所示。



添加完毕后，单击“确定”按钮，关键字 sum(就被添加到过滤规则列表内了，如果有用户向网站提交关键字 sum(，龙盾 IIS 防火墙将会拦截用户的访问。

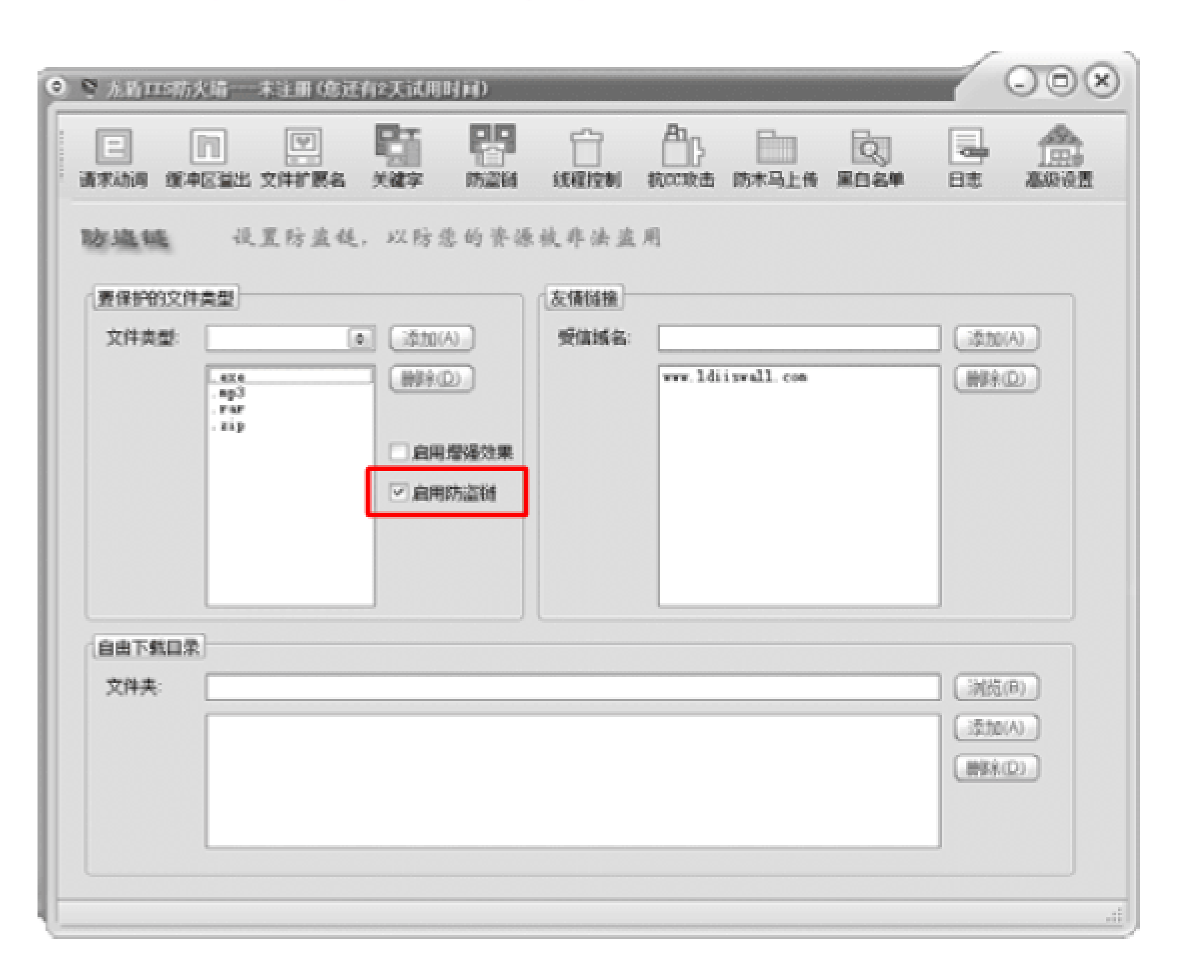

注 意 事 项

SQL 注入过滤规则的强度等级分为“低”和“高”两种。

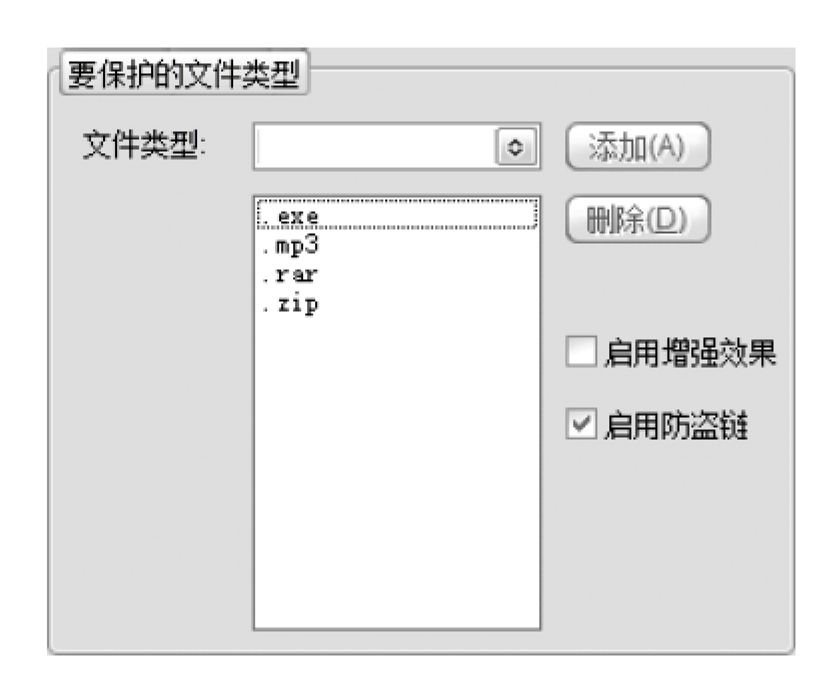
如果过滤强度选择“高”，则该条规则必须使用“正则表达式”，否则过滤可能会失效并引起错误。

技巧290 设置龙盾 IIS 防火墙防盗链

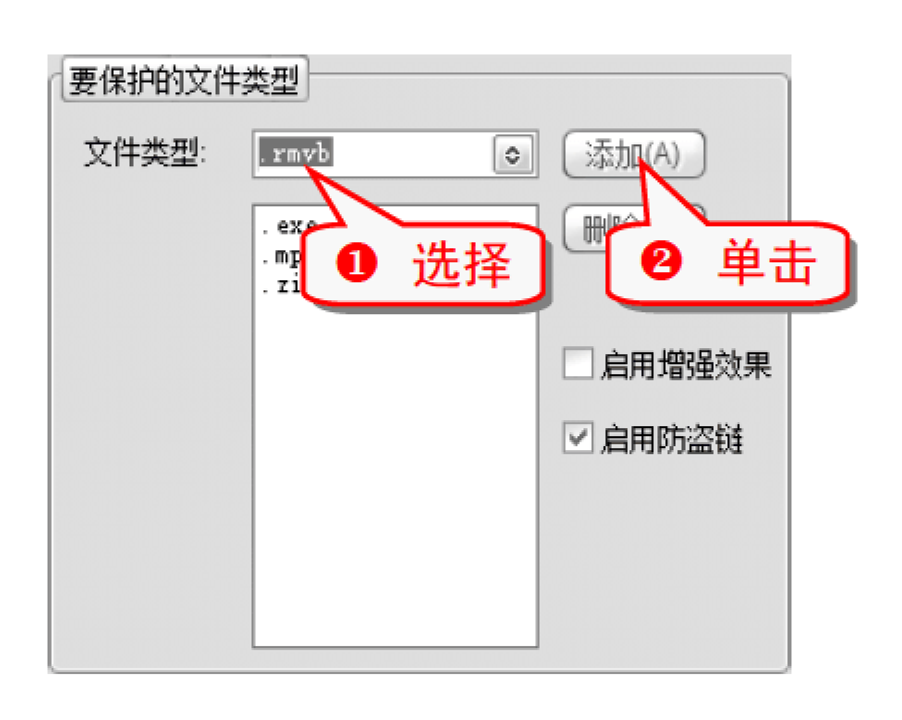
设置防盗链，可以保护网站上的资源不被非法链接，保护自己的资源不被非法下载，从而有效降低服务器数据的流量，增强服务器的稳定性。



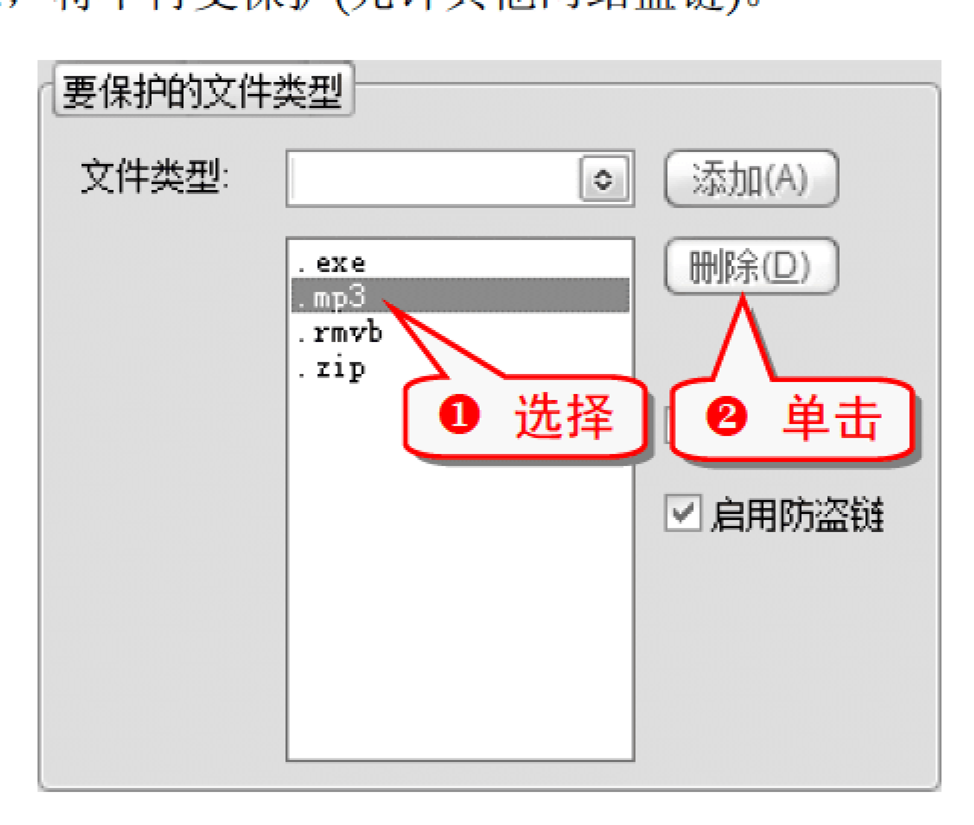
要保护的文件类型列表中指定类型的文件将被保护，即只有通过该网站下载，通过其他网站的链接将不能下载该资源。



添加要保护的文件类型的步骤如下。



可以根据需要“删除”被保护的类型，被删除类型的资源，将不再受保护(允许其他网站盗链)。



可以根据需要，选择“启用”或“停用”防盗链功能和增强效果。

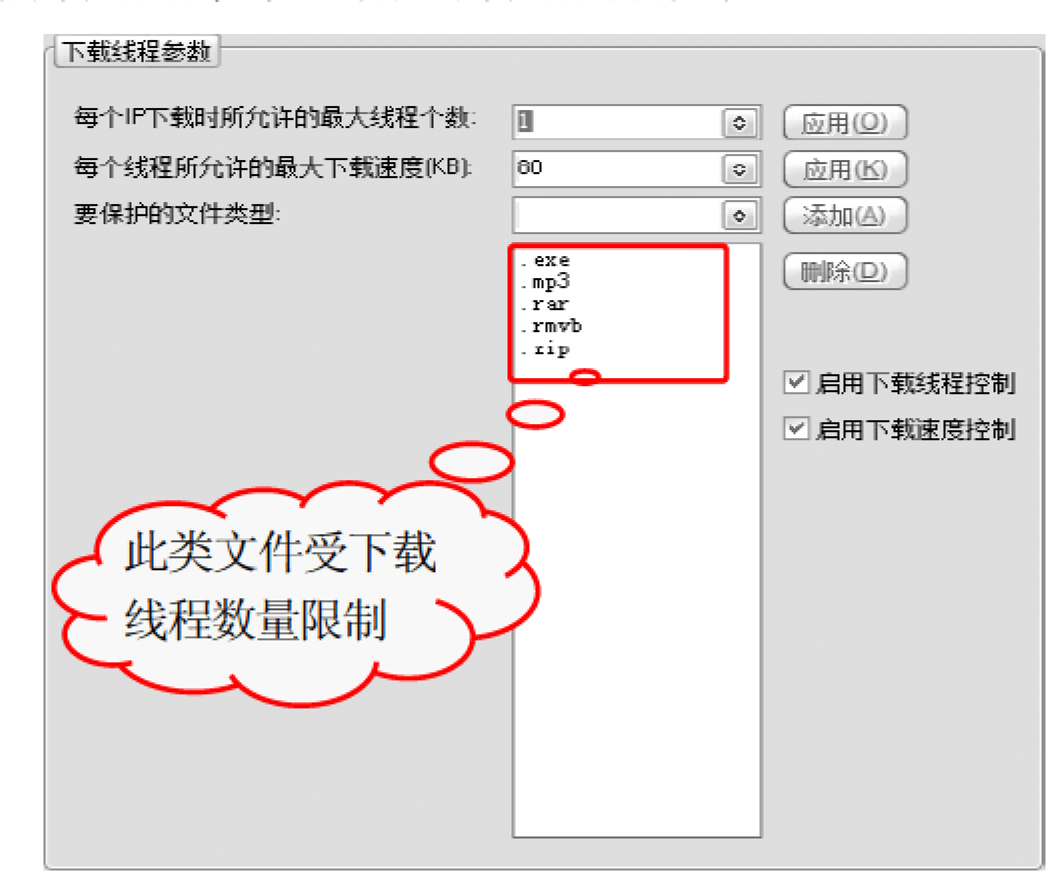

知 识 补 充

增强效果是指除了具备一般防盗功能，客户要想下载文件，还必须具备以下条件：只有用户在 10 分钟内登录过该网站，才允许下载该网站的文件，此功能可以有效抵御下载工具或用户伪造 Referer 字段，以提升防盗效果。可以根据实际情况，启用或停用该功能。



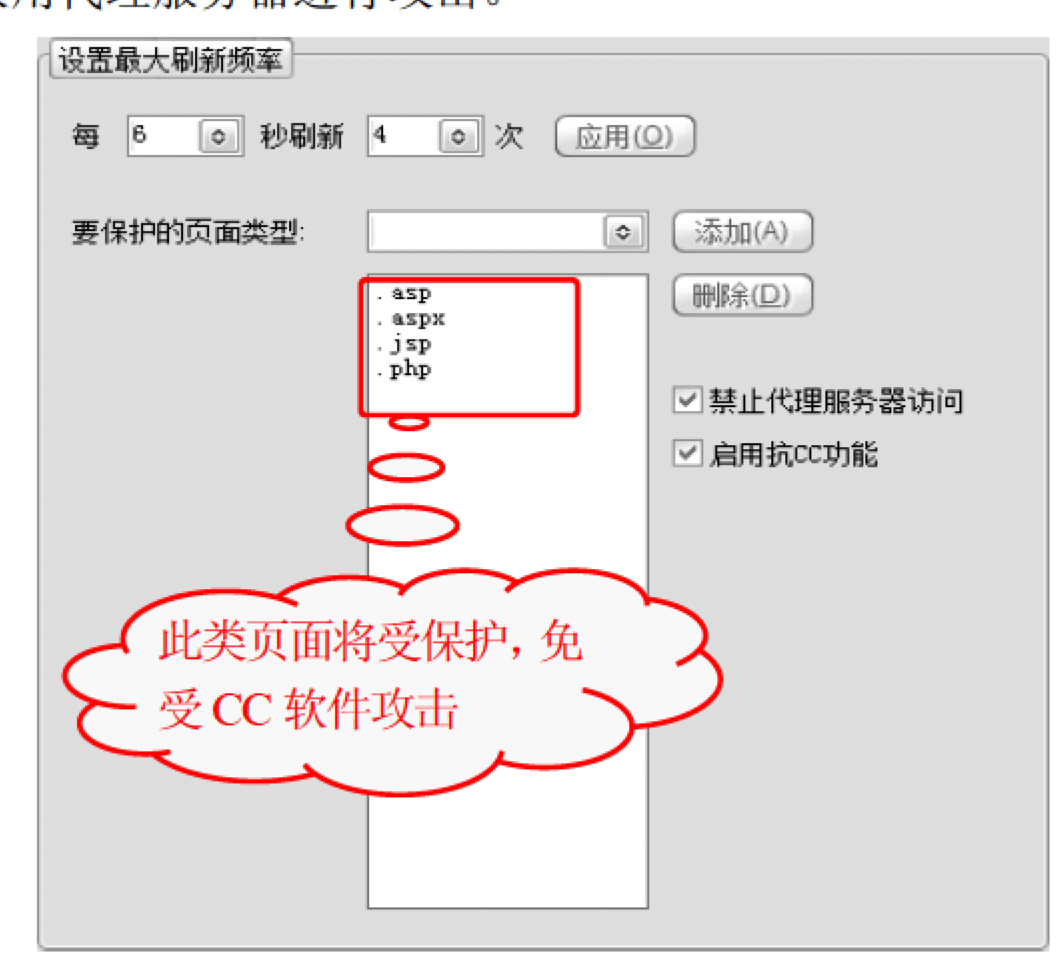
技巧291　设置龙盾 IIS 防火墙线程控制

线程控制的功能是控制文件下载的线程个数以及下载速度，降低网络流量，降低服务器的资源消耗，从而提高服务器的效率，增强服务器的稳定性。



技巧292　设置龙盾 IIS 防火墙抗 CC 攻击

“CC 攻击”是指利用 CC 软件对动态页面(.asp/.php 等)进行高频率访问，如果页面涉及关于数据库查询等比较消耗资源的操作，则大量的、高频率的访问会导致服务器陷入超级繁忙状态，最终导致拒绝服务，CC 软件一般采用代理服务器进行攻击。



可以根据实际情况，设置页面的刷新频率。

专　家　坐　堂

设置频率为“每 6 秒访问 4 次”：是指同一个访问者 IP，对同一个页面(比如：http://xxx.com/index.asp)，每 6 秒最多允许访问 4 次，如果超过这个访问频率(比如 5 次或更多)，则将禁止其访问，并记录此 IP，两小时内此 IP 将不能访问该页面，两个小时后将解除此限制。

技巧293　360ARP 防火墙

360ARP 防火墙是 360 安全卫士系列的安全小工具之一，适合局域网用户使用，可以有效拦截局域网中的 ARP 攻击，同时将第一时间对网关 MAC 的变更给予提示功能。



专　家　坐　堂

360ARP 防火墙的功能：

内核层双向拦截本机和外部 ARP 攻击，及时查杀 ARP 木马。

精准追踪攻击源 IP，方便及时查询攻击源。

拦截 DNS 欺骗，网关欺骗，IP 冲突多种攻击。

可自定义本机进程白名单。

拦截通知可自行选择是否提示，方便用户使用。

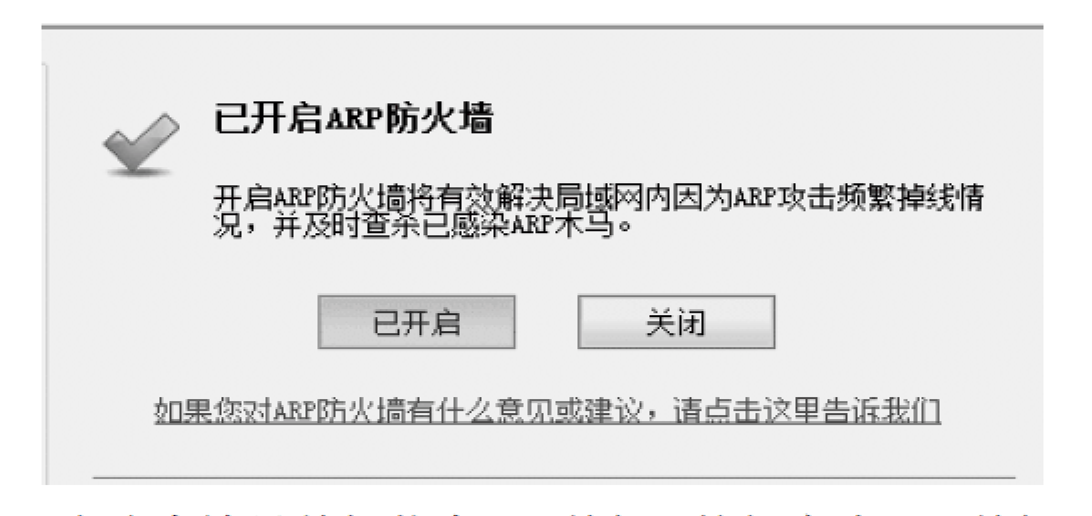
技巧294　开启 360ARP 防火墙的保护

“保护状态”选项卡中，左界面上记录着系统遭受 ARP 攻击以及防御的情况。

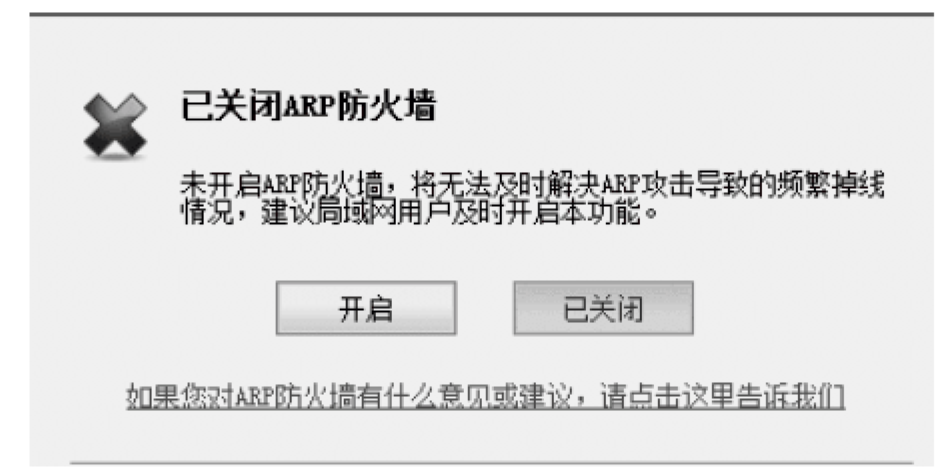


在该界面上可以设置防火墙的开启和关闭。

当防火墙呈开启状态，“开启”按钮变为“已开启”。

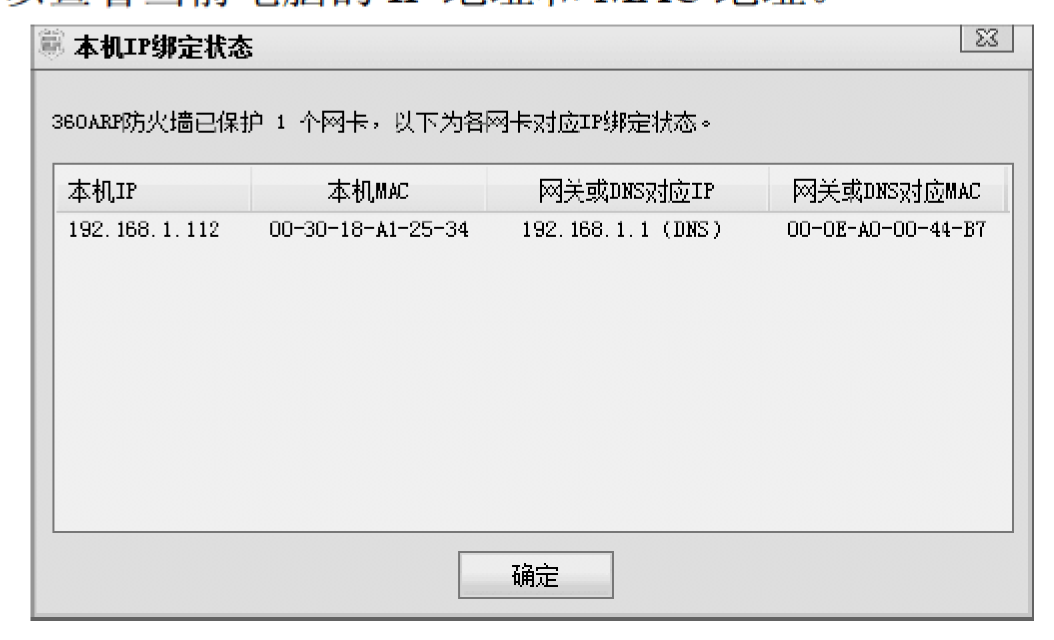


当防火墙呈关闭状态，“关闭”按钮变为“已关闭”。



单击 网关保护设置 按钮的功能是打开“综合设置”选项卡。

单击右下角的“查看本机 IP/MC 绑定状态”链接，可以查看当前电脑的 IP 地址和 MAC 地址。

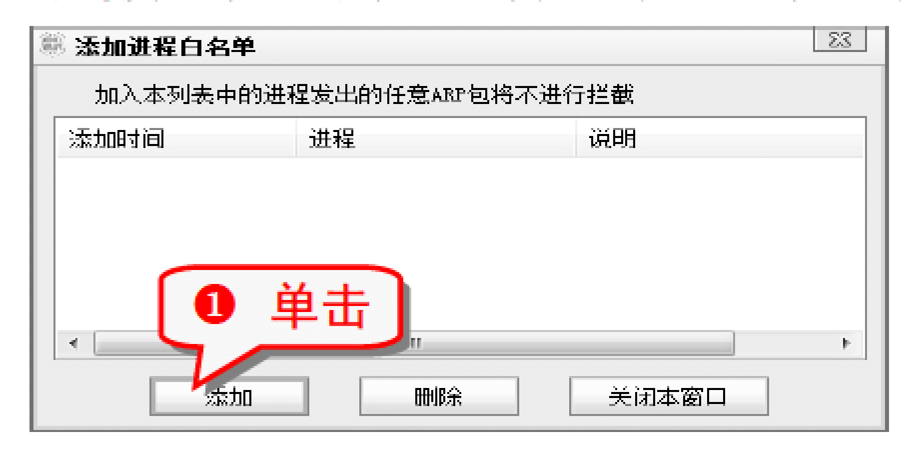


技巧295 综合设置 360ARP 防火墙

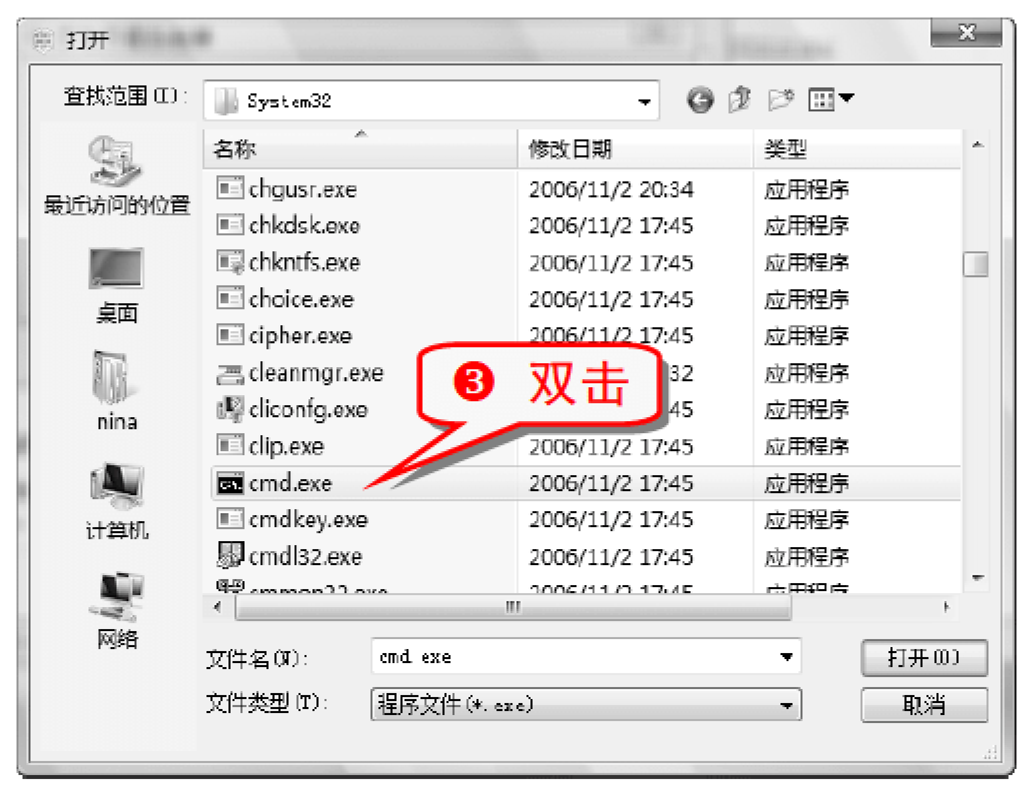
该选项卡中有“网关及 DNS/保护设置”、“拦截攻击类型设置”以及“拦截通知设置”3 个选项组，分别可以对网关及 DNS 保护方式、拦截攻击的类型和拦截通知的提示方式进行设置。



在“拦截攻击类型设置”选项组有一个“设置进程白名单”的链接，单击会弹出“添加进程白名单”对话框。











专题十一　木马病毒攻防战

内容导航

在木马和病毒日益猖獗的今天，网络安全形势严峻。其实只要了解木马和病毒的本质，掌握其攻击手段及伪装方法，清除木马和病毒将不再是个难题。

热点快报

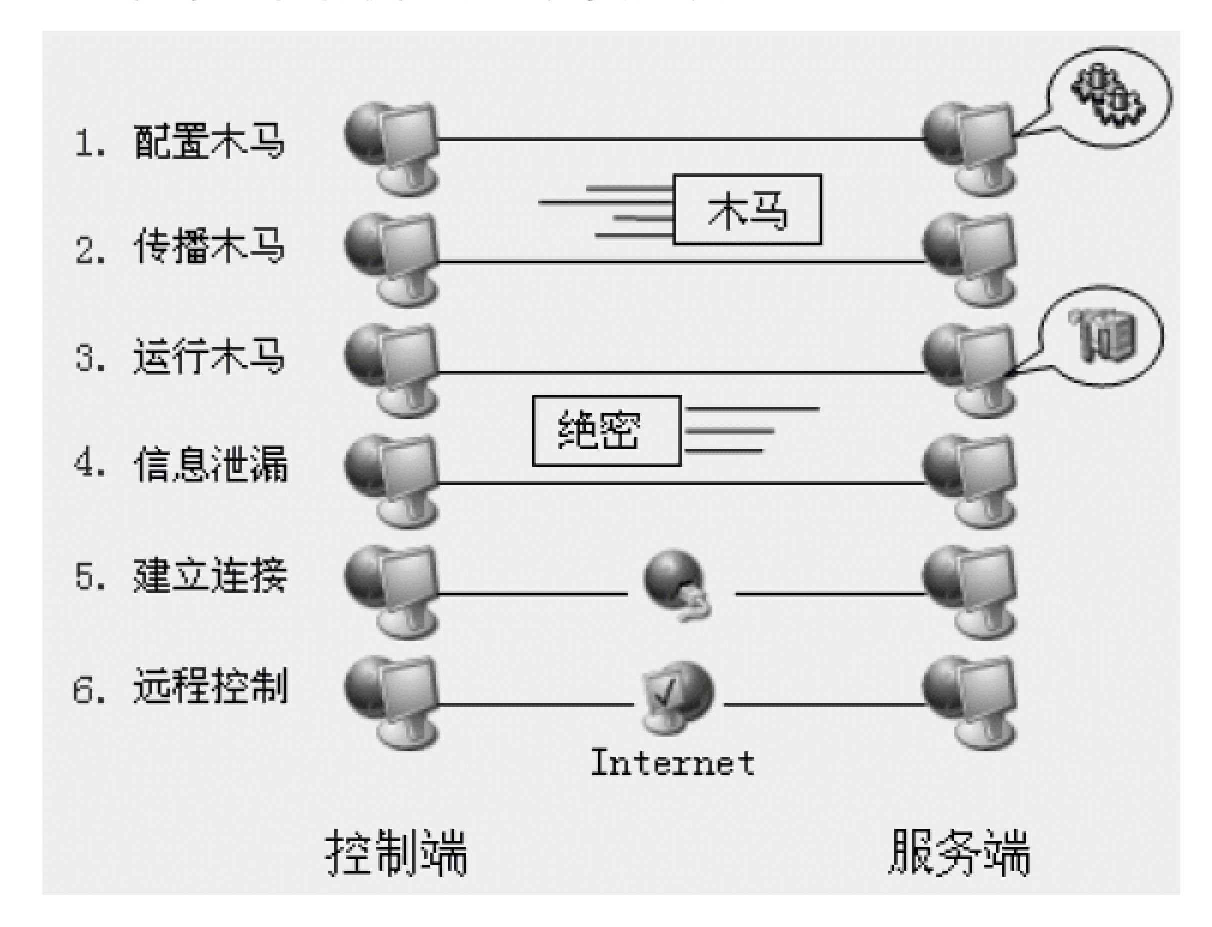
- 掌握加壳脱壳技术
- 认识木马伪装面具
- 清除 QQ 盗号木马
- 清除灰鸽子木马
- 手动查杀隐藏木马
- 常用病毒专杀工具

技巧296　揭开木马的神秘面纱

木马又称为特洛伊木马，英文名是 Trojan Horse，是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点，可以对电脑系统进行远程控制和窃取密码、控制系统、进行文件操作等破坏性操作。

一般的木马都有客户端和服务端两个执行程序。通常被植入了木马的电脑称为木马的服务端，而黑客控制的电脑称为木马的客户端。客户端用于黑客远程控制植入木马的电脑，而服务端程序就是通常所说的木马程序。

木马通常采取如下流程实施攻击。



专　家　坐　堂

木马，又被称为特洛伊木马，传说古希腊人围攻特洛伊城，久久不能得手，就想出一个木马计，让士兵藏在巨大的木马中，然后将木马丢弃于特洛伊城下假装撤退，让敌人将其作为战利品拖入城内。木马中的士兵则乘晚上敌人庆祝胜利、放松警惕的时候从木马中爬出来，与城外的部队里应外合攻下特洛伊城。

技巧297　常见的木马分类

(1) 破坏型

这种木马专门破坏并删除文件，能够自动删除目标电脑上的 DLL、INI、EXE 文件，一旦被感染就会严重威胁到电脑的安全。

(2) FTP 木马

这种木马是最简单和古老的木马，其唯一功能就是打开 21 端口等待连接。新 FTP 木马还加上了密码功能，这样只有木马植入者才知道正确的密码，才能够进入对方电脑。

(3) 代理木马

这种木马给被控制的电脑植入代理木马，可以让其变成攻击者发动攻击。通过代理木马，黑客可以在匿名的情况下使用 Telnet、ICQ、IRC 等程序，从而隐蔽自己的踪迹。

(4) 密码发送型

这种木马可以找到目标电脑的隐藏密码，在受害者不知道的情况下，把密码发送到指定的信箱。

(5) 远程访问型

这种木马是使用最广泛的木马，可以远程访问被攻击者的硬盘。

(6) 键盘记录木马

这种木马可以随着 Windows 的启动而启动，有在线和离线记录两种选项，目标电脑上按过什么按键，黑客可以从记录中知道，并从中找出密码信息，甚至是信用卡账号。

(7) DOS 攻击木马

这种木马的危害不是体现在被感染电脑上，而是体现在被黑客利用来攻击一台又一台电脑，给网络造成很大的伤害。

(8) 反弹端口型木马

防火墙往往会对接入的链接进行非常严格的过滤，但对接出的链接却疏于防范。和一般的木马相反，反弹端口型木马的被控制端往往使用主动端口，控制端使用被动端口。

(9) 程序杀手木马

这种木马的功能是可以关闭对方电脑上运行的防木马程序，让其他的木马更好地发挥作用。

专 家 坐 堂

很多远程访问型木马都可以使用代理服务端的方式连接“肉鸡”，而且连接“肉鸡”后首先检查对方是否开启了防火墙，如果有，则杀掉其进程，这样有利于黑客隐藏身份，从而实现远程控制目的。

技巧298　加壳与脱壳技术

加壳是指对木马程序进行封装，以绕过安全软件的查杀。

(1) 木马的加壳

所谓加壳，是一种通过一系列数学运算，将可执行程序文件或动态链接库文件的编码进行改变，以达到缩小文件体积或加密程序编码的目的。当被加壳的程序运行时，外壳程序先被执行，然后由这个外壳程序负责将用户原有的程序在内存中解压缩，并把控制权交还给脱壳后的真正程序，一切操作自动完成。一般情况下，加壳程序和未加壳程序的运行结果是一样的。

众所周知，目前杀毒软件主要依靠特征码技术查杀木马和病毒。由于加壳软件会对源文件进行压缩、变形，使加密前后的特征码完全不同。脱壳能力不强的杀毒软件，对付“加壳”后木马就需要添加两条不同的特征记录。如果黑客换一种加壳工具加壳，则对于这些杀毒软件来说又是一种新的木马，必须添加新的特征记录才能够查杀。如果杀毒软件的脱壳能力较强，则可以先将木马文件脱壳，再进行查杀，这样只需要一条记录就可以对这些木马通杀，不仅减小杀毒软件对系统资源的占用，同时大大提升了其查杀木马和病毒的能力。

(2) 对木马进行脱壳

脱壳主要有两种方法：硬脱壳和动态脱壳。

硬脱壳：这是指找出加壳软件的加壳算法，写出逆向算法，就像压缩和解压缩一样。由于目前很多“壳”均带有加密和变形的特点，每次加壳生成的代码都不一样。使用硬脱壳往往不能起效，但由于其技术门槛较低，仍然被一些杀毒软件所使用。

动态脱壳：由于加壳的程序运行时必须还原成原始形态，即加壳程序会在运行时自行脱掉“外壳”。目前，有一种脱壳方式是抓取(Dump)内存中的镜像，再重构成标准的执行文件，相比硬脱壳方法，这种脱壳方法对自行加密、变形的壳处理效果更好。

技巧299　木马植入电脑的方法

木马要植入电脑，首先需要以一定的伪装措施骗过目标电脑的用户，传播至目标电脑上，然后再安装运行。

木马的传播方式主要有通过 E-mail 传播、软件下载传播以及 IE 浏览器传播三种类型。

(1) E-mail 传播

木马程序以附件的形式夹在邮件中发送出去，收信人只要打开附件就会感染木马。

(2) 软件下载传播

一些非正规的网站以软件下载为名，将木马捆绑在软件安装程序上，下载后只要一运行这些程序，木马即会自动安装。

(3) IE 浏览器传播

木马可以通过 Script、ActiveX 及 ASP、CGI 交互脚本的方式植入，由于 IE 浏览器在执行 Script 脚本时存在安全漏洞，木马可以很容易植入被攻击的电脑。

知 识 补 充

木马还可以利用一些系统漏洞植入，如 IIS 服务端溢出漏洞，通过一个 IISHACK 攻击程序使 IIS 服务端崩溃，同时在服务端上执行木马程序，从而植入木马。



技巧300　木马的伪装面具

木马要成功地植入目标电脑中，需要进行一定的伪装。目前木马的伪装手段主要有伪装成一般软件和绑定到正常程序两大类型。

(1) 伪装成一般软件

用户经常可以在网站上发现一些很好玩的小程序，下载执行后系统却报告内部错误导致程序退出。这时一般都会认为是程序没有开发好，不会怀疑运行了木马程序。等到运行自己的QQ等程序时，被告知密码不正确，才会检查自己的电脑是否被安装了木马。

这种程序实质就是木马伪装成的，通过在木马代码的前段完成自我安装与隐藏的过程，最后显示“软件错误信息”，以达到欺骗的目的。

(2) 绑定到正常程序

一些黑客通过捆绑软件把一个正版的安装程序和木马捆绑成一个新的程序，用户在安装该正版程序时，就被神不知鬼不觉地植入木马。



专　家　坐　堂



通常用的木马伪装工具有网页木马生成器、万能文件捆绑器和合成工具 Exe binder 等。

技巧301　木马喜欢的藏身之处

(1) 集成到程序中

木马常常集成到程序里，一旦木马程序被激活，木马文件就会和某一应用程序捆绑在一起，覆盖源文件，这样即使木马被删除了，只要运行捆绑了木马的应用程序，木马又会被安装上去。如果木马捆绑到系统文件中，则Windows系统每次启动都会启动木马。

(2) 隐藏在配置文件中

木马经常藏身于不太重要的配置文件中，利用配置文件的特殊作用，木马很容易就能在电脑中运行，从而进行偷窥和监视。

(3) 潜伏在 Win.ini 中

木马要想达到控制或者监视电脑的目的，必须要处于运行状态。Win.ini 是一个既安全又能在系统启动时自动运行的区域。

(4) 伪装在普通文件中

把可执行文件伪装成图片或文本，即在程序中把图标改成 Windows 的默认图片图标，再把文件名改为*.jpg.exe，由于 Windows Vista 默认设置是“不显示已知的文件后缀名”，文件将会显示为*.jpg，双击图标就中木马了。

(5) 内置到注册表中

注册表比较复杂，是木马最喜欢的藏身之处，不易被发现，又能自动运行。

(6) 隐藏在 System.ini 中

Windows 安装目录下的 System.ini 也是木马喜欢隐蔽的地方。打开这个文件，在该文件的[boot]字段中，如果有 shell=Explorer.exe file.exe 这样的内容，这里的 file.exe 就是木马服务端程序。

(7) 隐形于启动组中

有时木马只在乎能否自动加载到系统中，因为一旦木马加载到系统中，无论用什么方法都不能将其删除，因此，启动组也是木马藏身的好地方。

(8) 隐蔽在 Winstart.bat 中

Winstart.bat 也是一个能自动被 Windows 加载运行的文件，多数情况下为应用程序及 Windows 自动生成，于是也成了木马喜欢隐蔽的地方。

(9) 捆绑在启动文件中

黑客利用启动文件能启动程序的特点，将制作好的带有木马启动命令的同名文件上传到服务端覆盖同名文件，这样就可以达到启动木马的目的。

(10) 设置在超级链接中

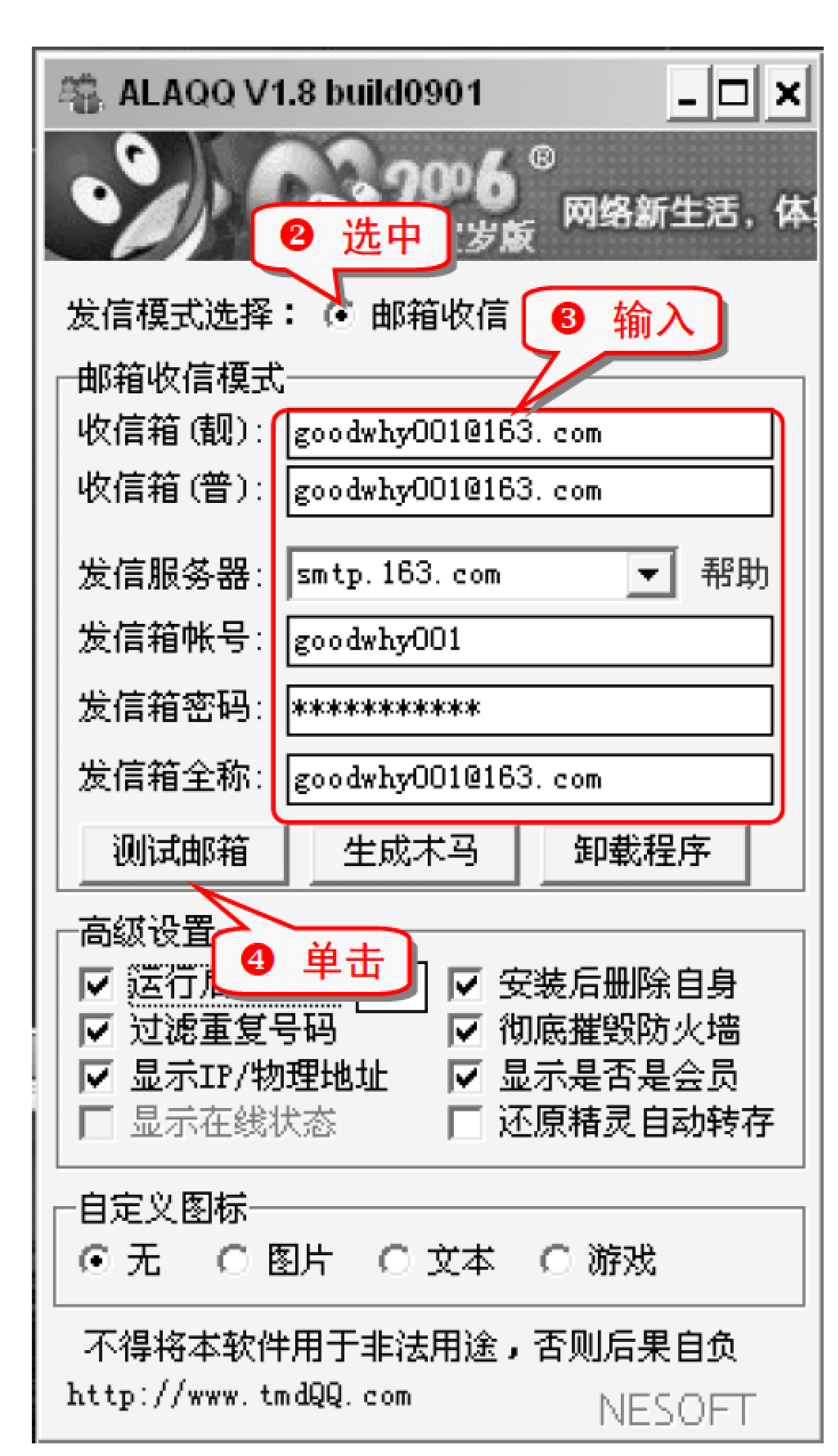
木马传播者在网页上放置恶意代码，引诱用户点击，导致电脑中木马。

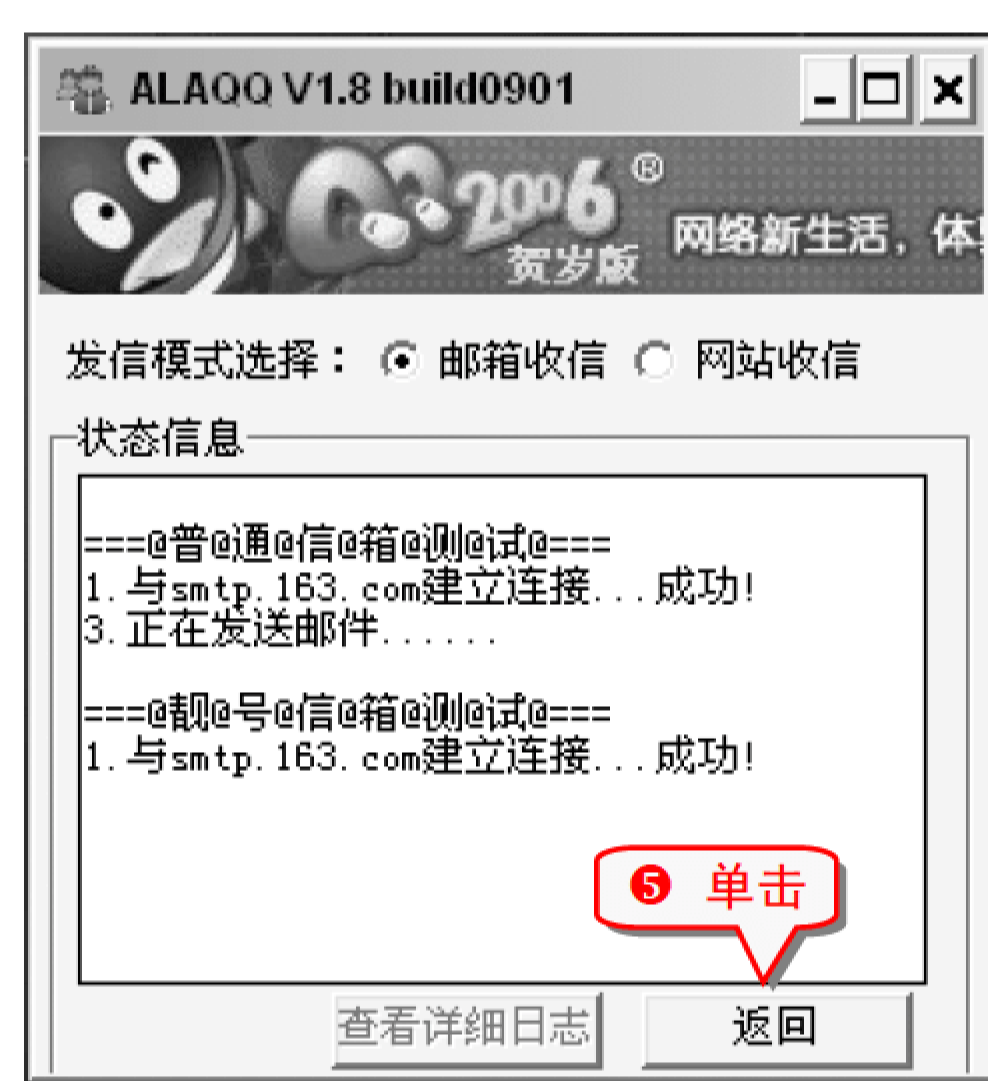
技巧302　“啊拉 QQ 大盗”盗号原理

“啊拉 QQ 大盗”的压缩包中有一个以.exe 为后缀名的文件和以.asp 为后缀名的文件，.exe 为后缀名的文件是“啊拉 QQ 大盗”的配置程序，.asp 为后缀名的文件是使用“网站收信”模式时需要使用的文件。

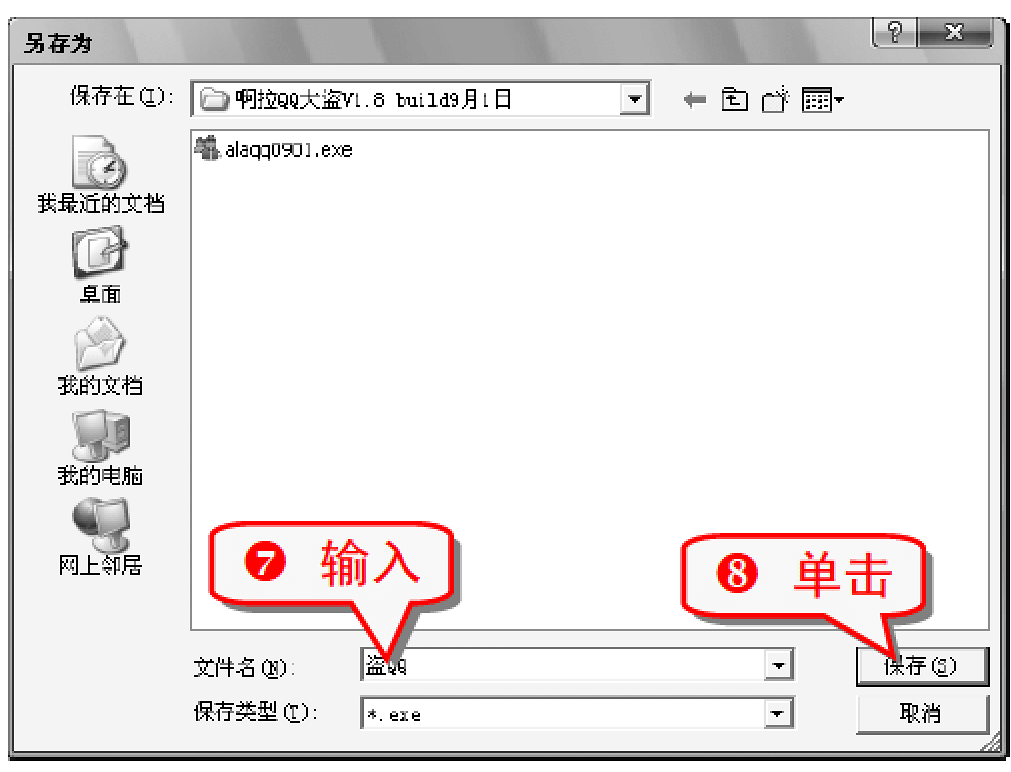
盗号者有两种方式可以接收被盗的 QQ 信息，分别是“邮箱收信”和“网站收信”形式，其通常都会选择“邮箱收信”，下面介绍通过“邮箱收信”盗取 QQ 的过程。

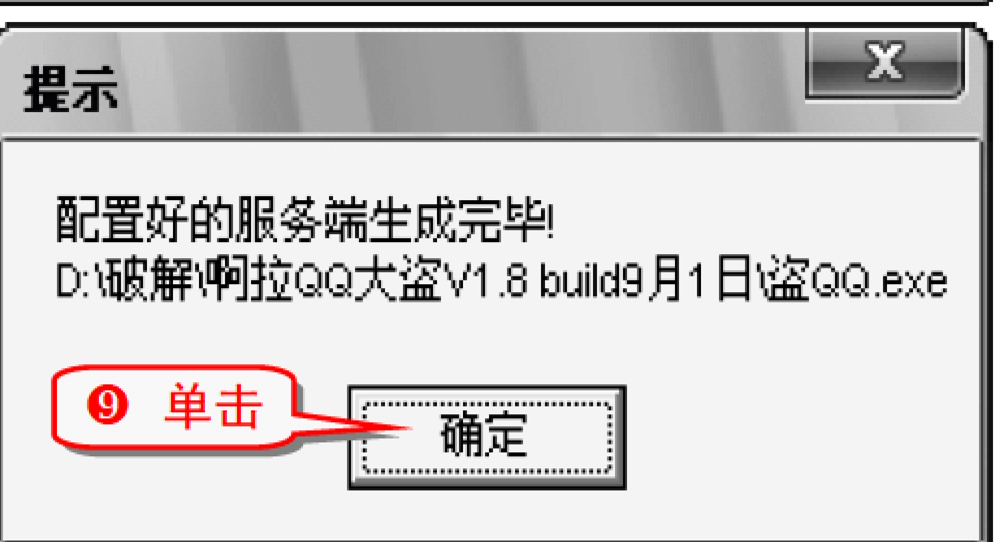
❶ 双击.exe 为后缀名的文件，弹出如下对话框。





❻ 返回到主配置界面，单击“生成木马”按钮。





❿ 生成一个能盗取 QQ 号码的木马程序。



举 一 反 三

“网站收信”模式是让被盗取的 QQ 信息自动上传到指定的网站空间中。

如果是在网吧里使用该木马，需要将“还原精灵自动转存”复选框选中，这样系统重新启动后仍能运行木马。

专 家 坐 堂

在“高级设置”下面如果选中“运行后关闭 QQ”复选框，当目标电脑运行“啊拉 QQ 大盗”生成的木马时，QQ 程序会在 60 秒后自动关闭，当对方再次登录 QQ 时，木马就会将登录的 QQ 号码以及密码都截获，并发送到盗号邮箱里去。

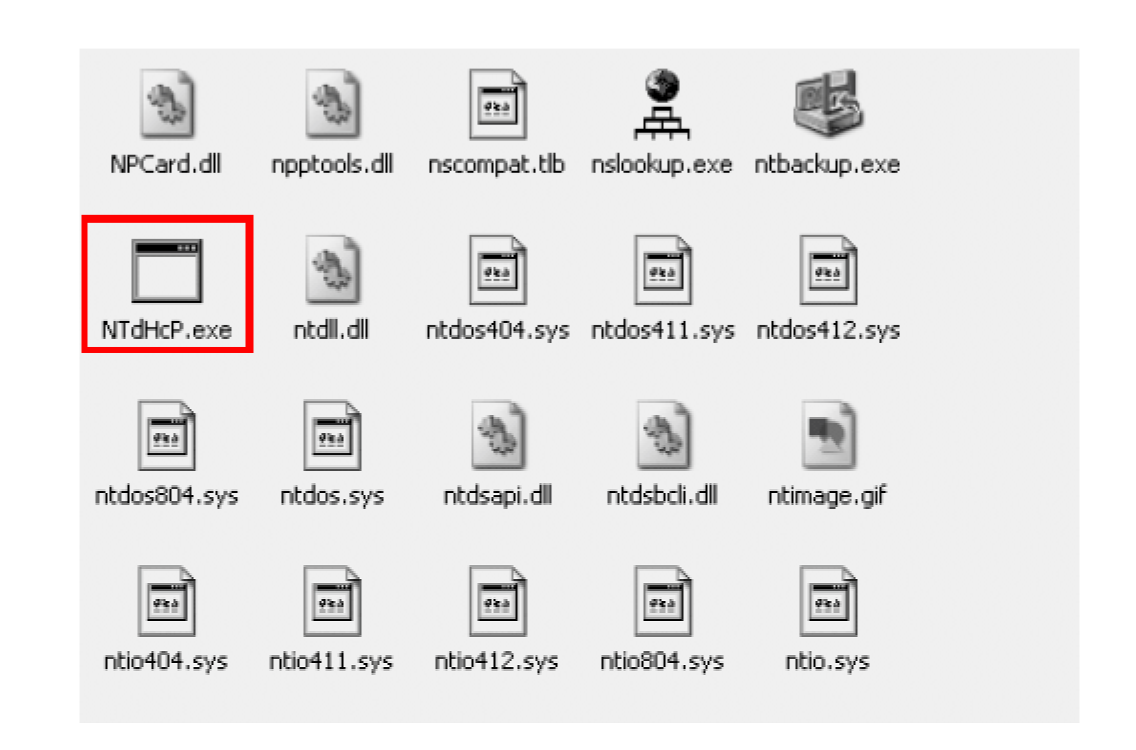


技巧303　检查自己是否中了“啊拉 QQ 大盗”

在上一个技巧中了解了“啊拉 QQ 大盗”盗取 QQ 号码的基本流程，那如何检查自己的电脑是否中了“啊拉 QQ 大盗”呢？

如果遇到以下几种情况，则表示被植入病毒。

- 运行一个小程序时，自动消失。
- 在登录 QQ 时，QQ 运行程序自动关闭。
- 打开 C 盘 Windows 目录中的 system32 文件夹下有一个名为 NTdHcP.exe 的文件。



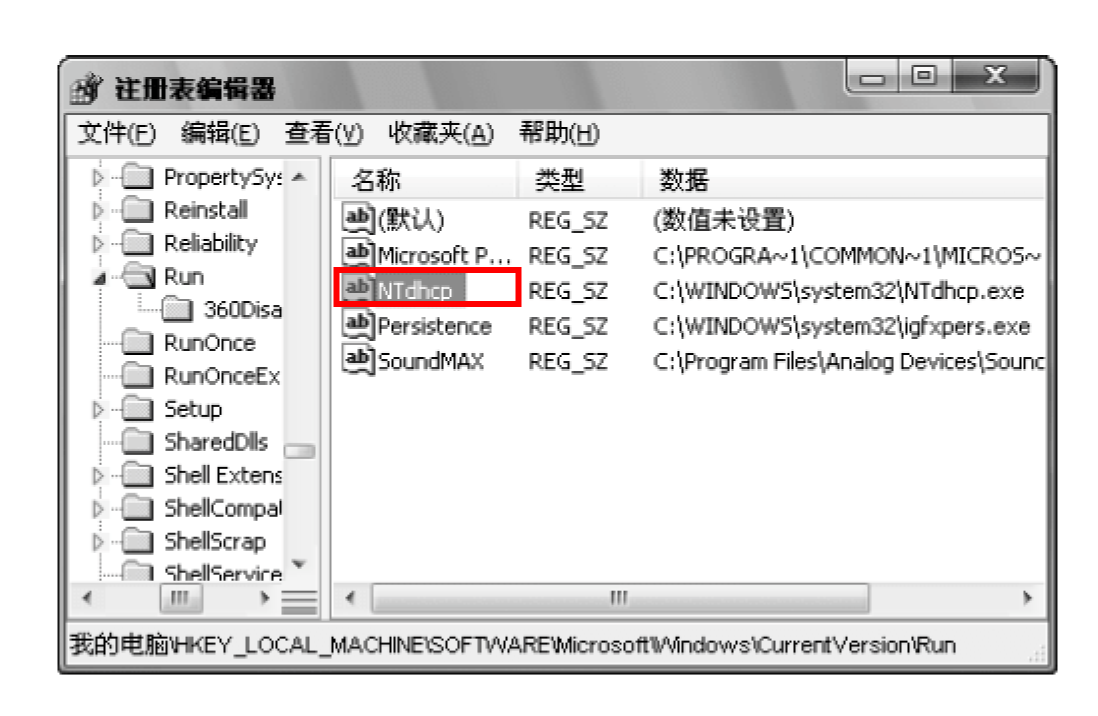
注　意　事　项

将系统隐藏的文件都显示出来，才能找到该文件。

- 打开“Windows 任务管理器”窗口，发现有 NTdHcP.exe 这个进程的存在。



- 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 分支，发现有一个名为 NTdhcp 的键值存在。



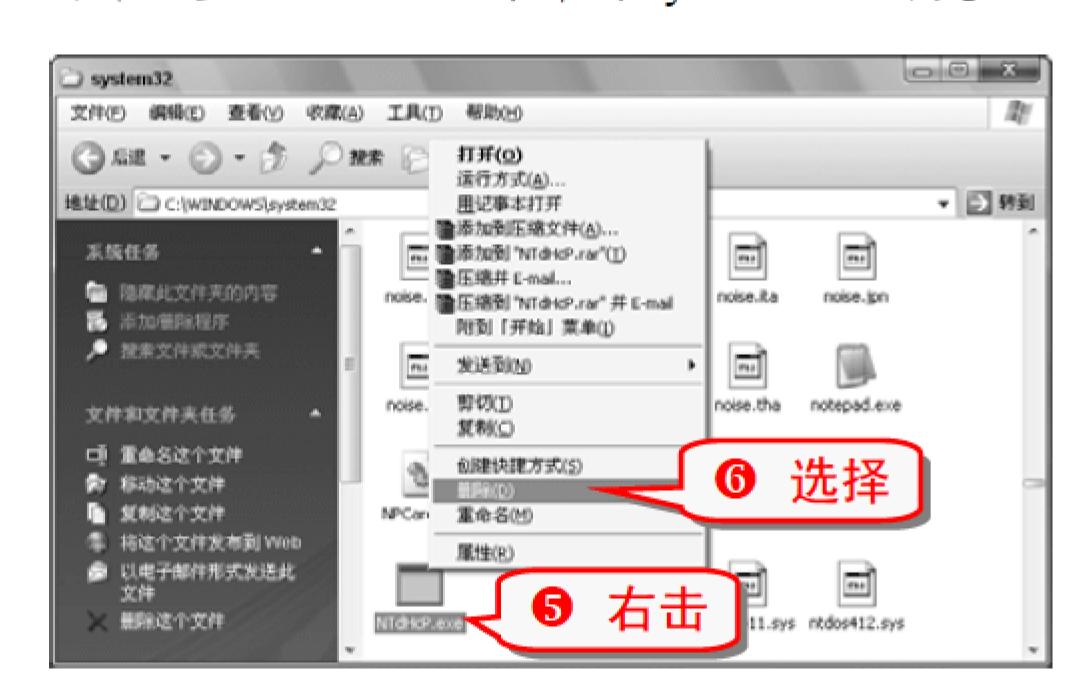
技巧304　手动删除“啊拉 QQ 大盗”

发现系统中了“啊拉 QQ 大盗”木马后，可以手动将其清除。

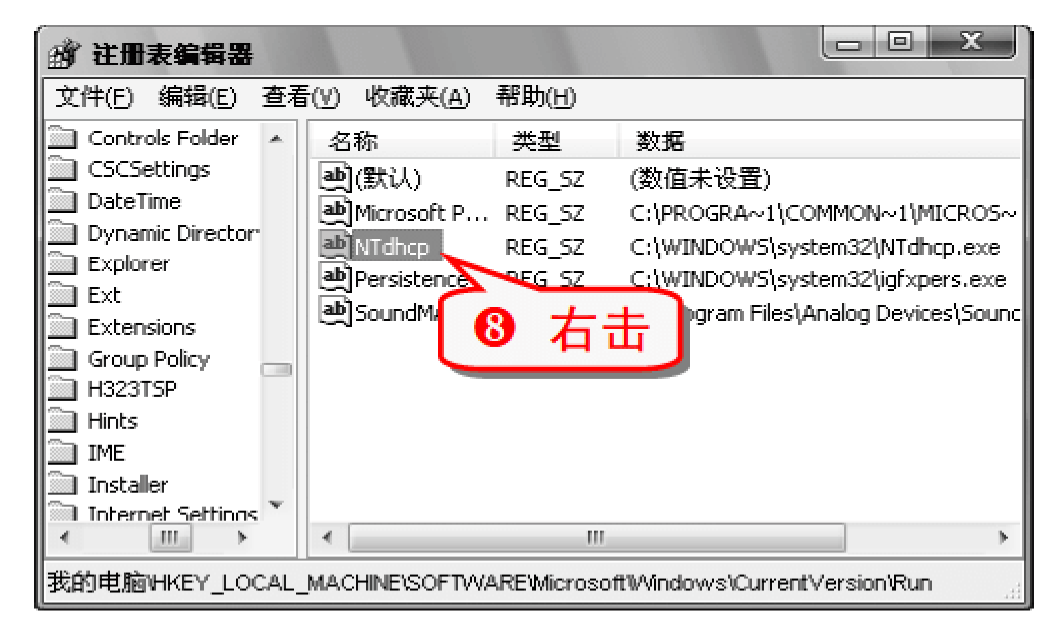
❶ 打开“Windows 任务管理器”窗口。

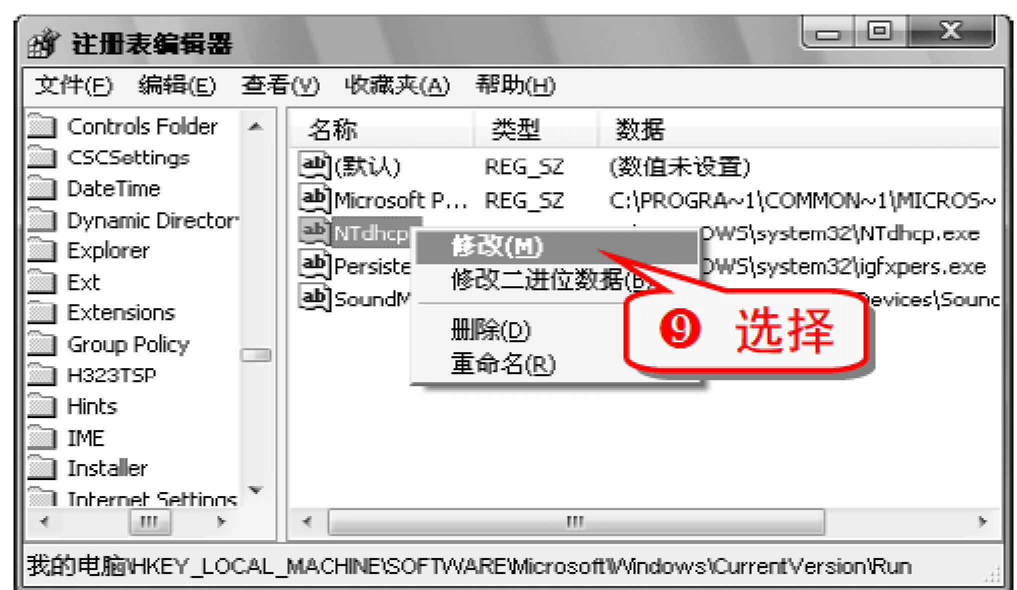


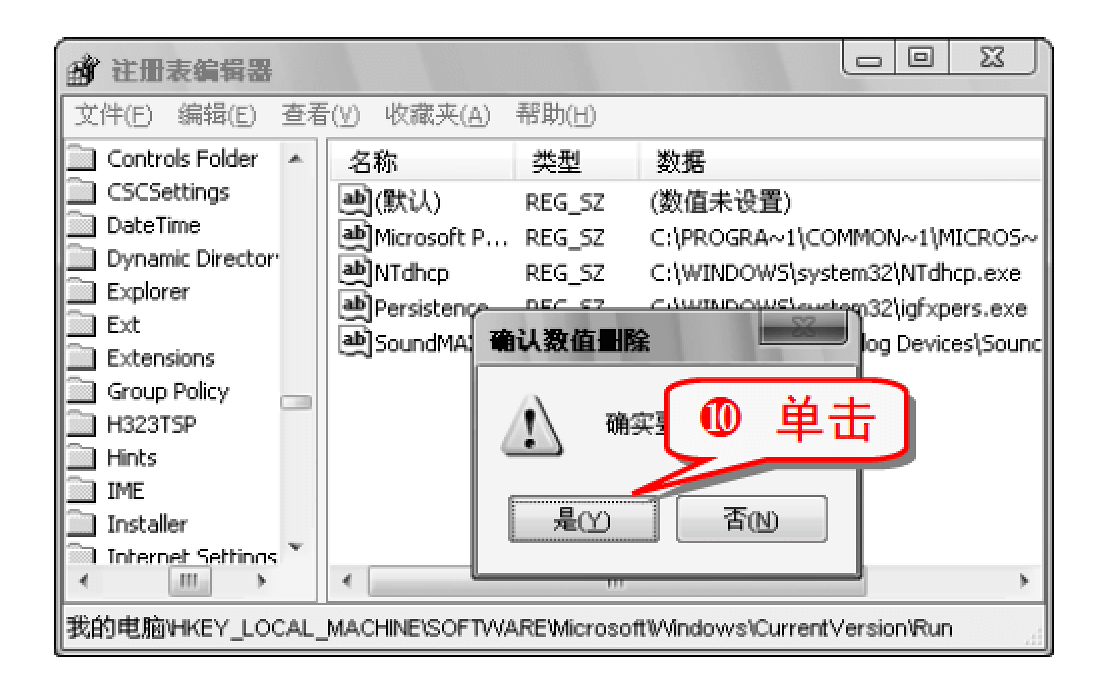
❹ 打开 C 盘 Windows 目录中的 system32 文件夹。



❼ 打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 分支。



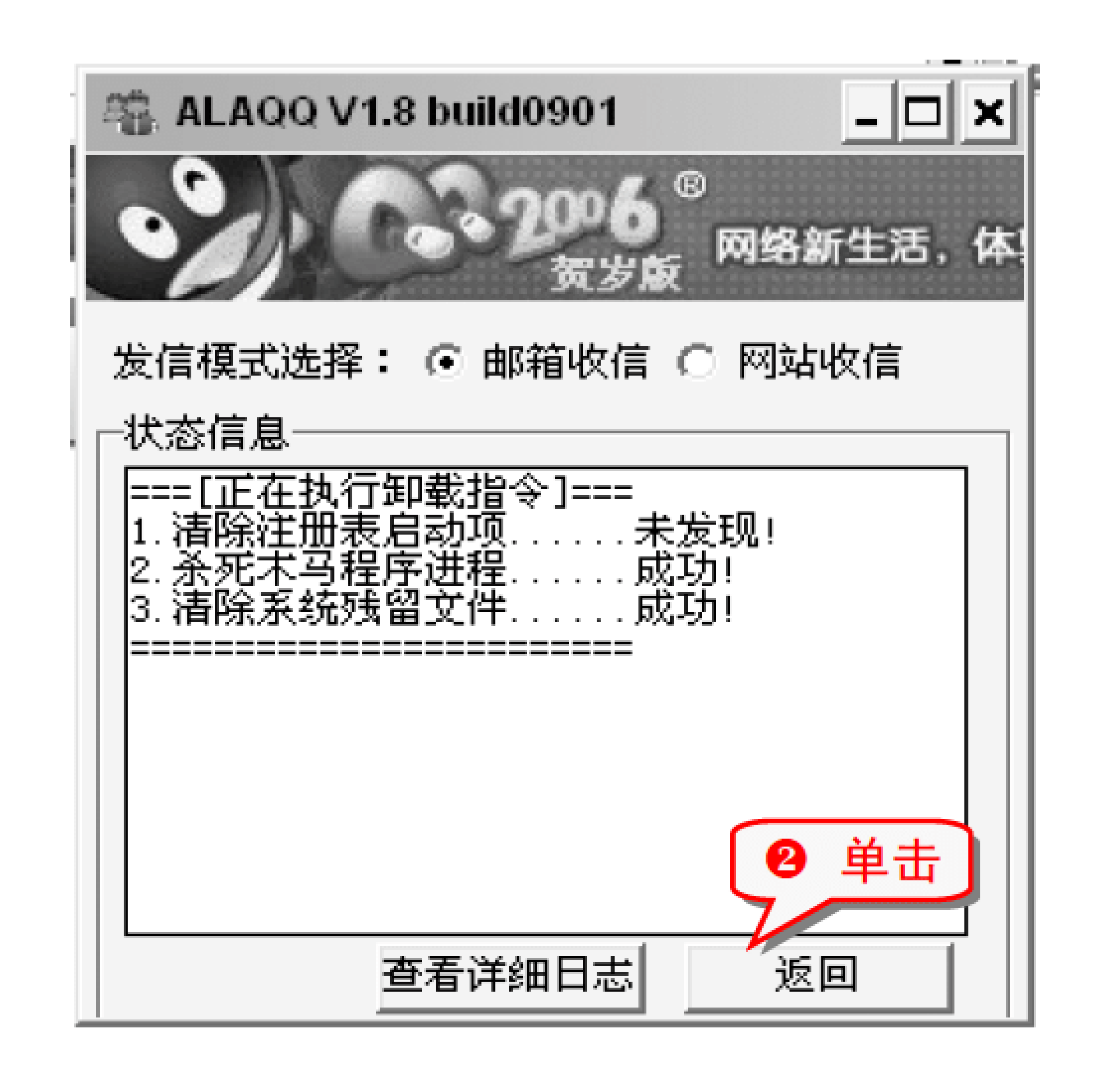




技巧305 强制卸载“啊拉 QQ 大盗”

只要拥有“啊拉 QQ 大盗”的配置程序，也就是“啊拉 QQ 大盗”压缩包中以.exe 为后缀名的文件就可以将“啊拉 QQ 大盗”木马完全清除出系统。





技巧306 利用 x-sniff 反夺盗号者邮箱

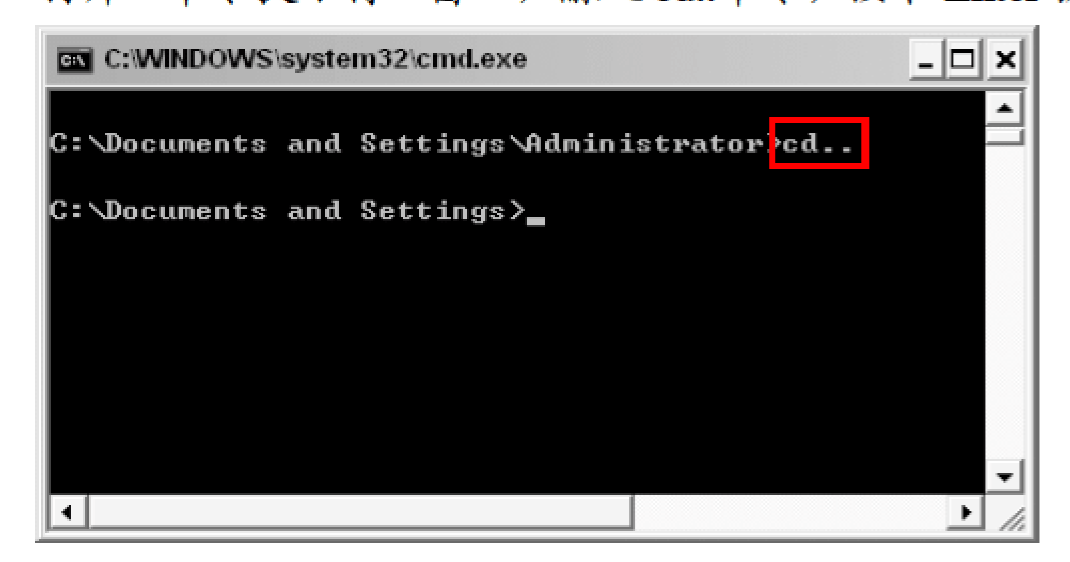
知道电脑中了“啊拉 QQ 大盗”木马，可以先不着急清除木马。

之前已经了解了“啊拉 QQ 大盗”木马盗号的过程，可以知道盗号者如果想要通过邮箱的方式获得被盗的 QQ 和密码，则必须在配置部分填写收取 QQ 号码信息的邮箱帐号和密码，而这些信息都保存在木马程序中。这样就可以通过 x-sniff 嗅探工具截获盗号者的邮箱账号和密码。

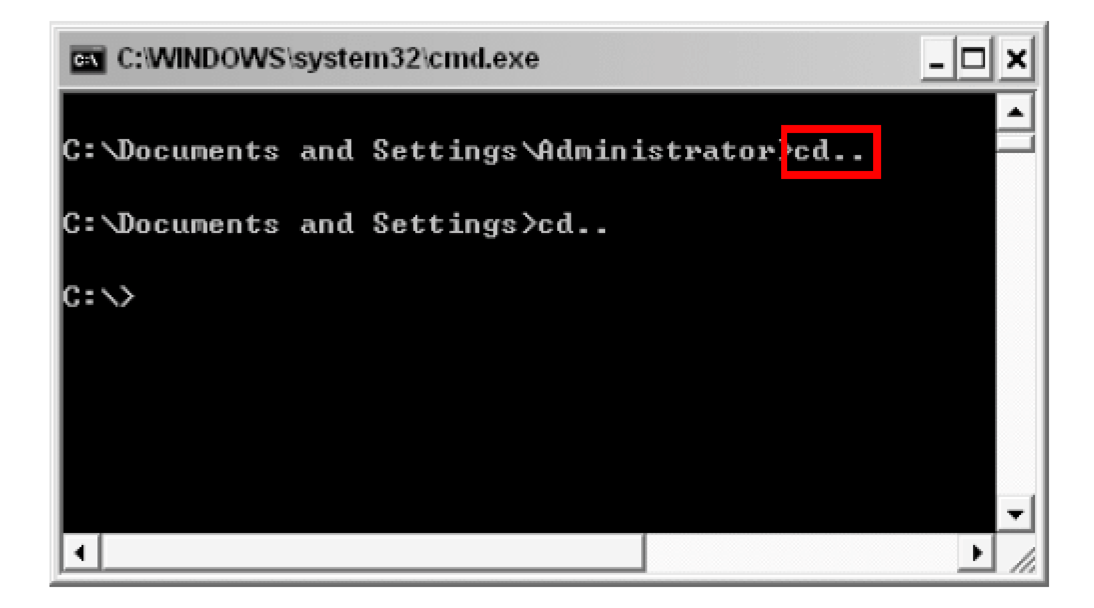
❶ 下载一个 x-sniff 工具包。

❷ 将其解压缩在 C 盘的根目录下，在 C 盘的根目录下会出现一个 xsniff.exe 文件和 xsniff.txt 文件。

❸ 打开“命令提示符”窗口，输入 cd..命令，按下 Enter 键。

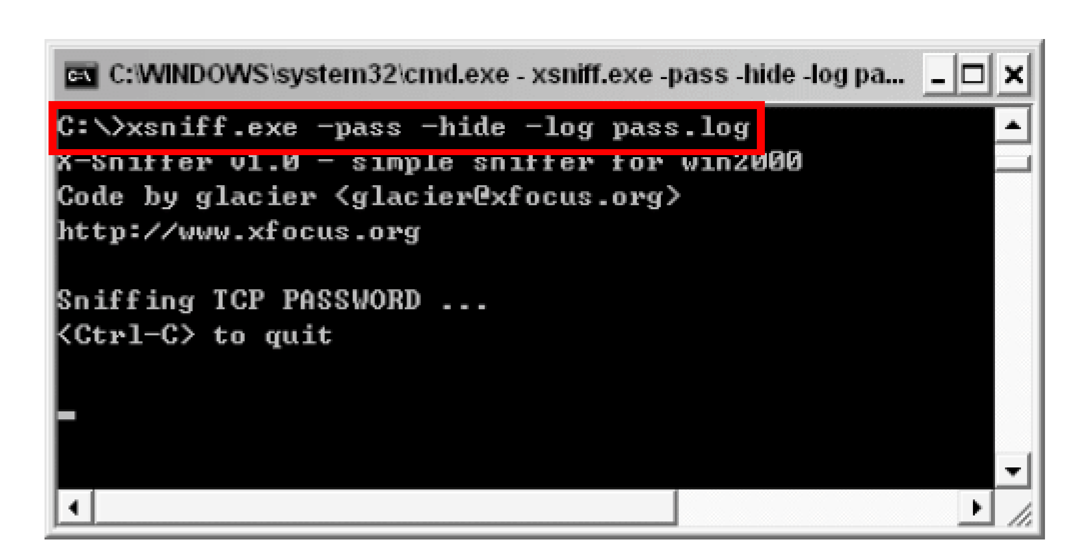


❹ 继续输入 cd..命令，按下 Enter 键。





❺ 输入 xsniff.exe -pass -hide -log pass.log 命令，按下 Enter 键。

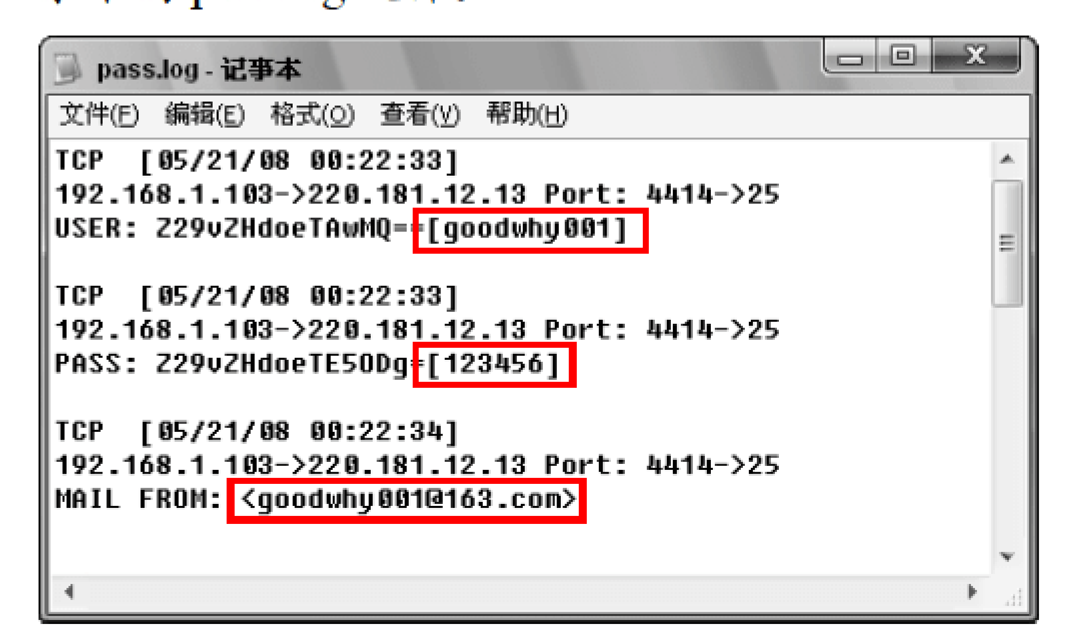




知 识 补 充

xsniff.exe -pass -hide -log pass.log 命令的意思是在系统后台运行 xsniff.exe，过滤出截获的数据包中的密码信息，并将这些密码信息保存到同目录下的 pass.log 文件中。

❻ 正常登录一个无用的 QQ，过一段时间打开 C 盘根目录下的 pass.log 文件。



❼ 在 pass.log” 中可以找到盗号者邮箱的用户、密码以及完整的邮箱地址。




注 意 事 项

x-sniff 工具包不一定要解压在 C 盘的根目录下，路径可以由自己选择，在“命令提示符”中只要能进入 xsniff.exe 文件所在的目录下，就能运行 xsniff.exe -pass -hide -log pass.log 命令。

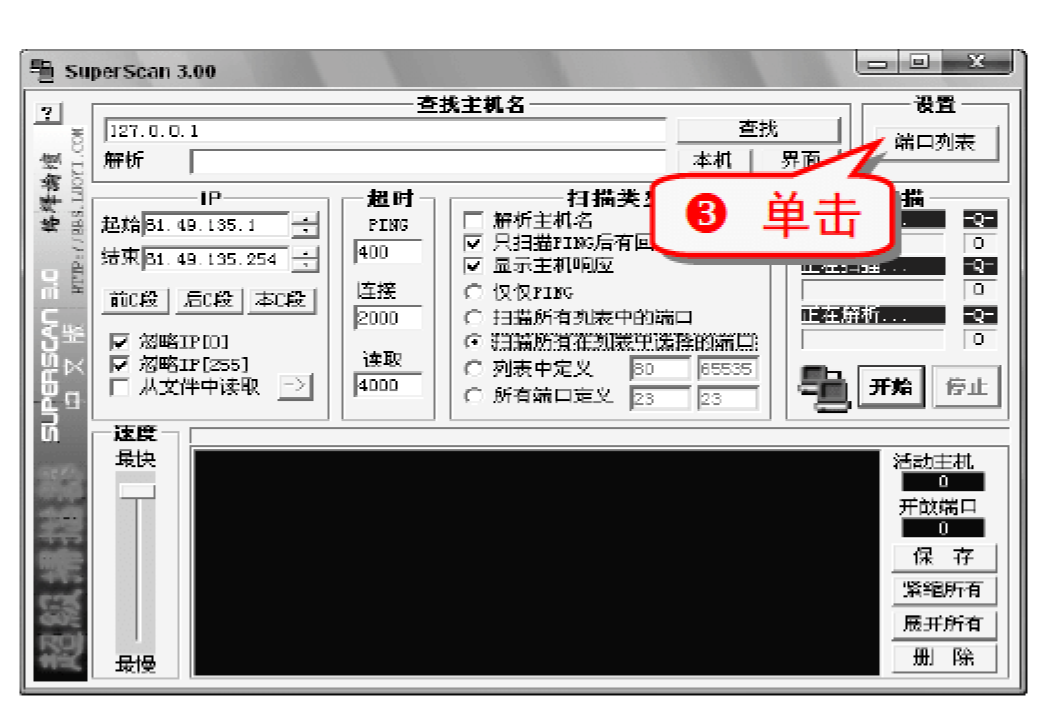
技巧307　防范远程盗取 ADSL 账号

黑客经常利用 ADSL 用户没有修改路由器默认密码这一漏洞，远程盗取 ADSL 账号和密码。下面揭露黑客是怎样进行攻击的。

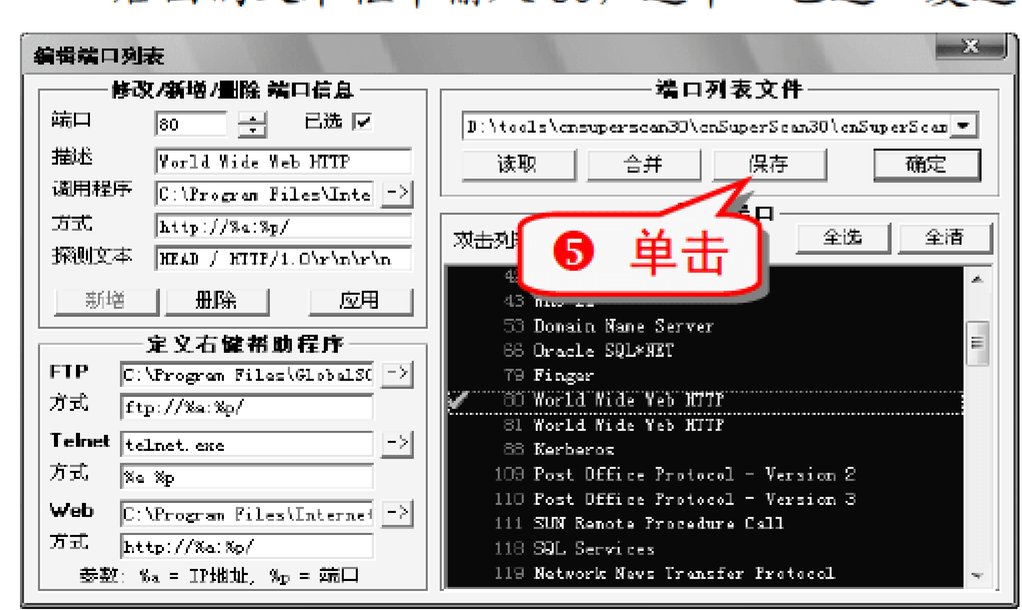
(1) 扫描端口 80 的主机

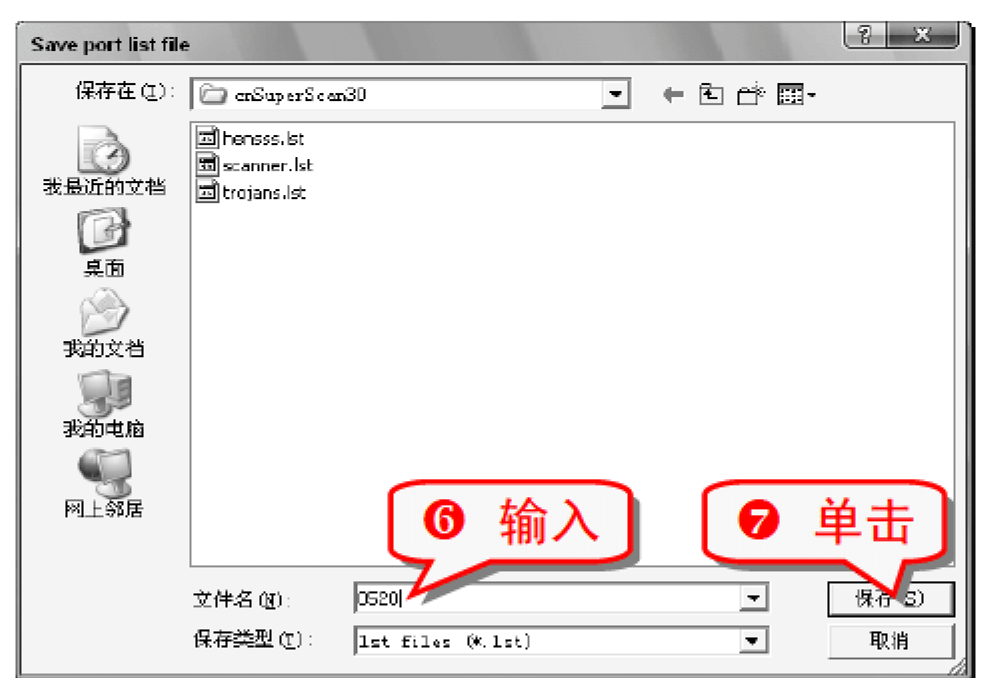
❶ 运行端口扫描工具 SuperScan 3.00。

❷ 在 IP 选项组中的“起始”和“结束”文本框中输入一段合法的 IP 地址扫描范围，在“扫描类型”选项组中选中“扫描所有在列表中选择的端口”单选按钮。



❹ 在弹出的“编辑端口列表”对话框中，单击“全清”按钮，然后双击选中 World Wide Web HTTP，在“端口”后面的文本框中输入 80，选中“已选”复选框。

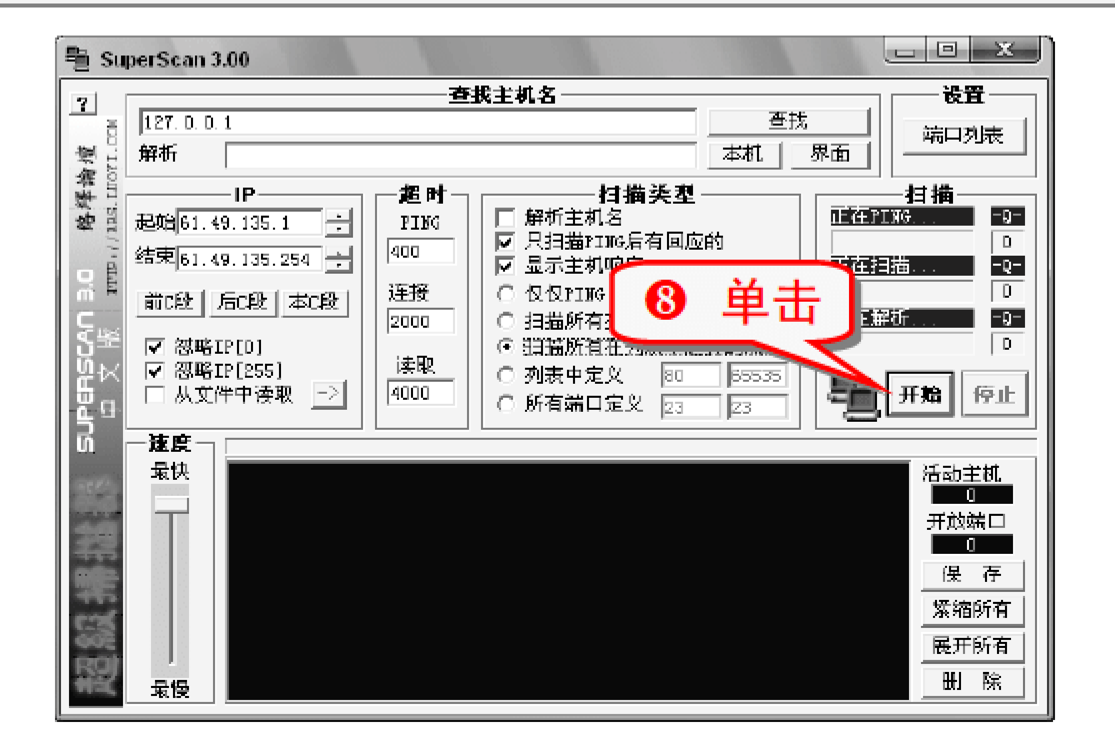






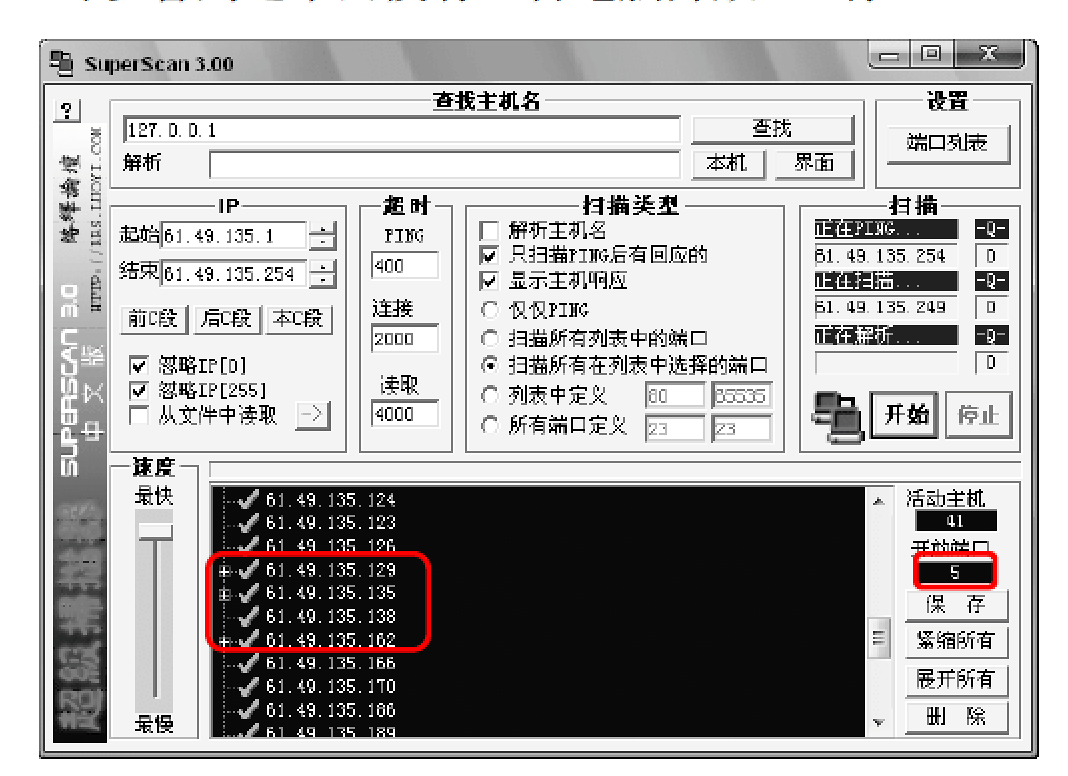
注 意 事 项

有时在单击“端口列表”按钮弹出的“编辑端口列表”中找不到端口 80 的扫描服务，这时可以单击“读取”按钮，选择不同的列表。

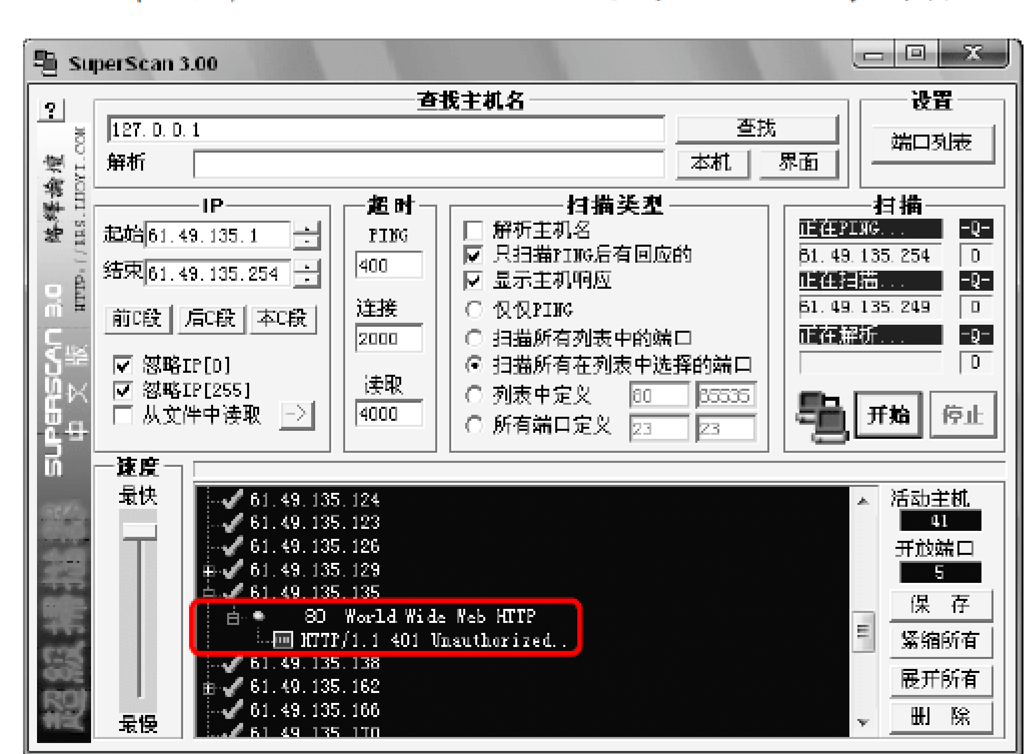


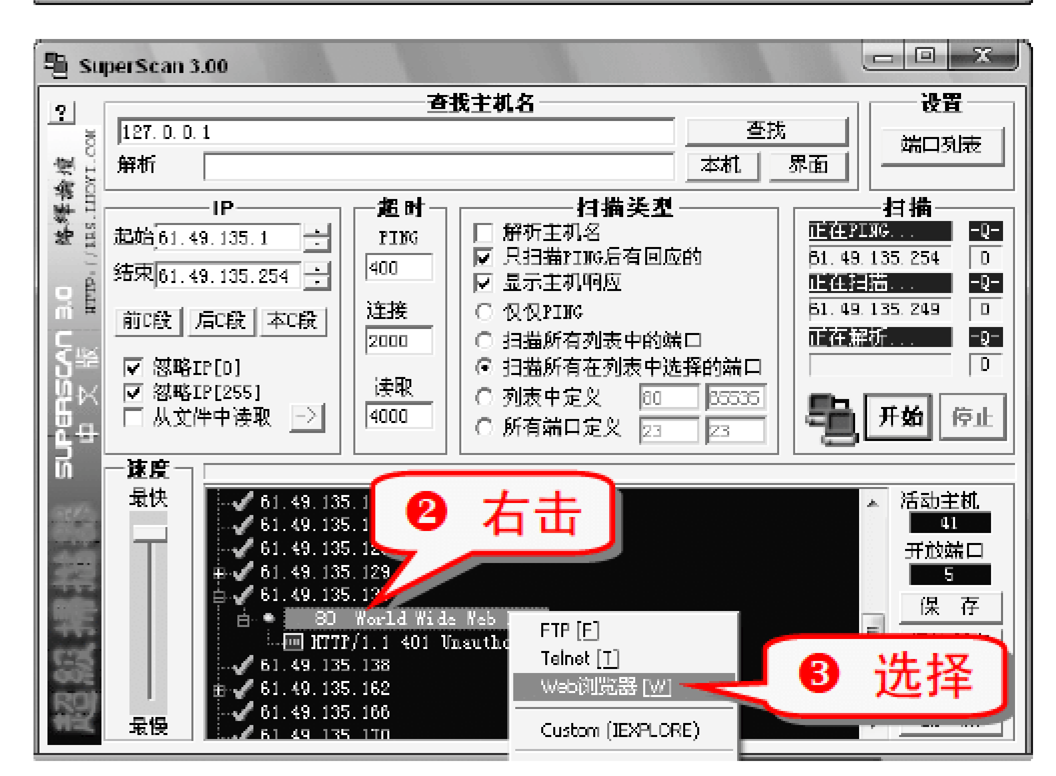
(2) 远程登录路由器

可以看到这个网段有5台电脑开放80端口。

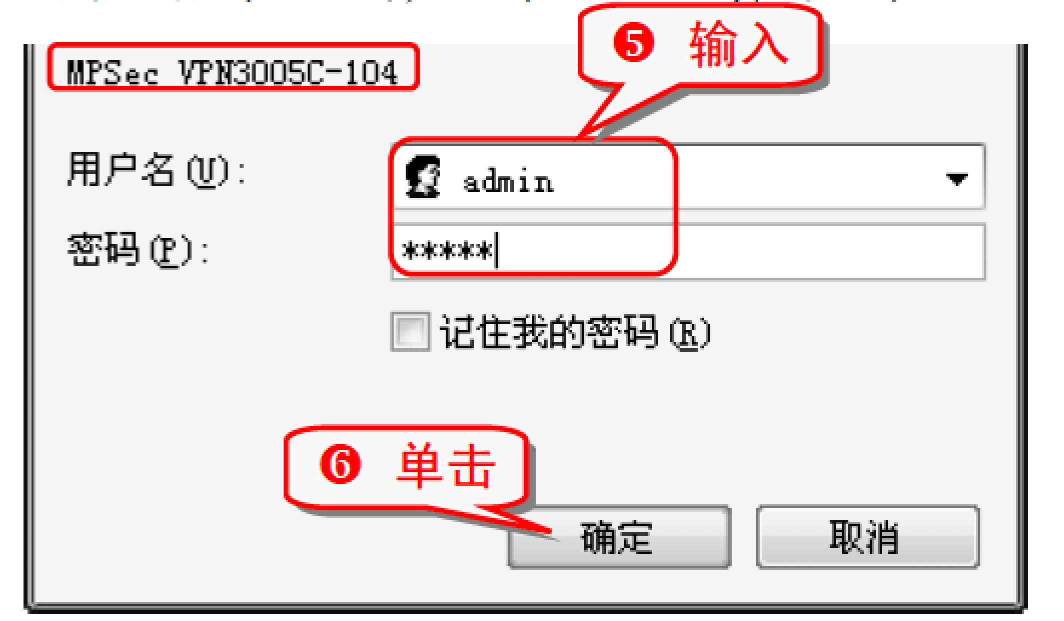


❶ 单击开放端口IP地址左边的小“+”号图标。





❹ 通过登录对话框上的路由器提示信息可以在网上查到该路由器的默认用户名为admin，密码也为admin。





路由器品牌与用户名及密码的对应如下表所示。

路由器品牌	默认用户名	默认密码
TP-LINK TD-8800	root	root
华为 MT800	admin	admin
Viking	root	root
Adsl Router	anonymous	12345
神州数码/华硕	adsl	adsl1234
eTEK 伊泰克 TD-SR400	Admin	Admin
艾玛 701H	admin	epicrouter
全向	root	root
大亚 DB102	admin	dare

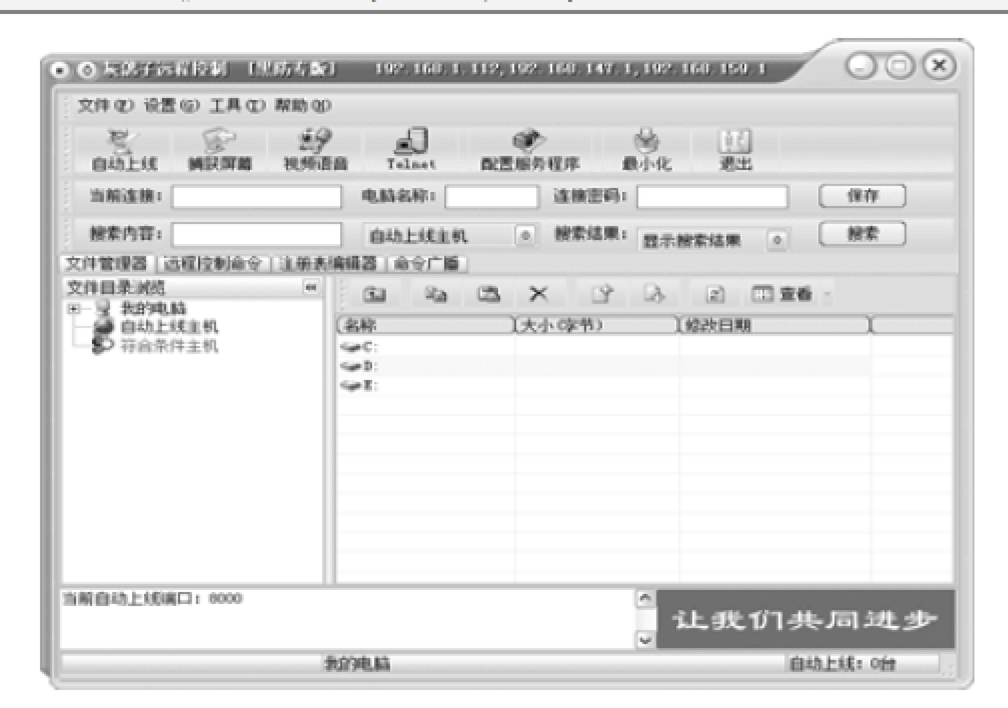
技巧308 合理应用灰鸽子木马

灰鸽子在正当使用的情况下，是一款很优秀的远程控制软件，如果用于不正当途径，灰鸽子便成了一款强大的入侵工具。现在灰鸽子是一款很强大的木马软件之一。

专 家 坐 堂

灰鸽子木马的特色功能。

- 穿透性强：以IE浏览器的身份主动连接客户端，而防火墙不会限制IE浏览器浏览网页，所以灰鸽子的穿透力强。
- 隐蔽性高：灰鸽子的服务端是由客户端自定义设置生成的，服务端安装成功后自动删除安装程序，并且伪装进程，在任务管理器中是无法找到其踪影的，其服务端安装程序的图标是可以修改的。
- 功能强大：拥有一般远程控制软件的功能，还可以查看被控制电脑的系统信息和剪切板上的信息，并控制其进程和服务，将其设置为一台代理服务器，以便控制对方的鼠标和键盘以及模拟注册表编辑器等。





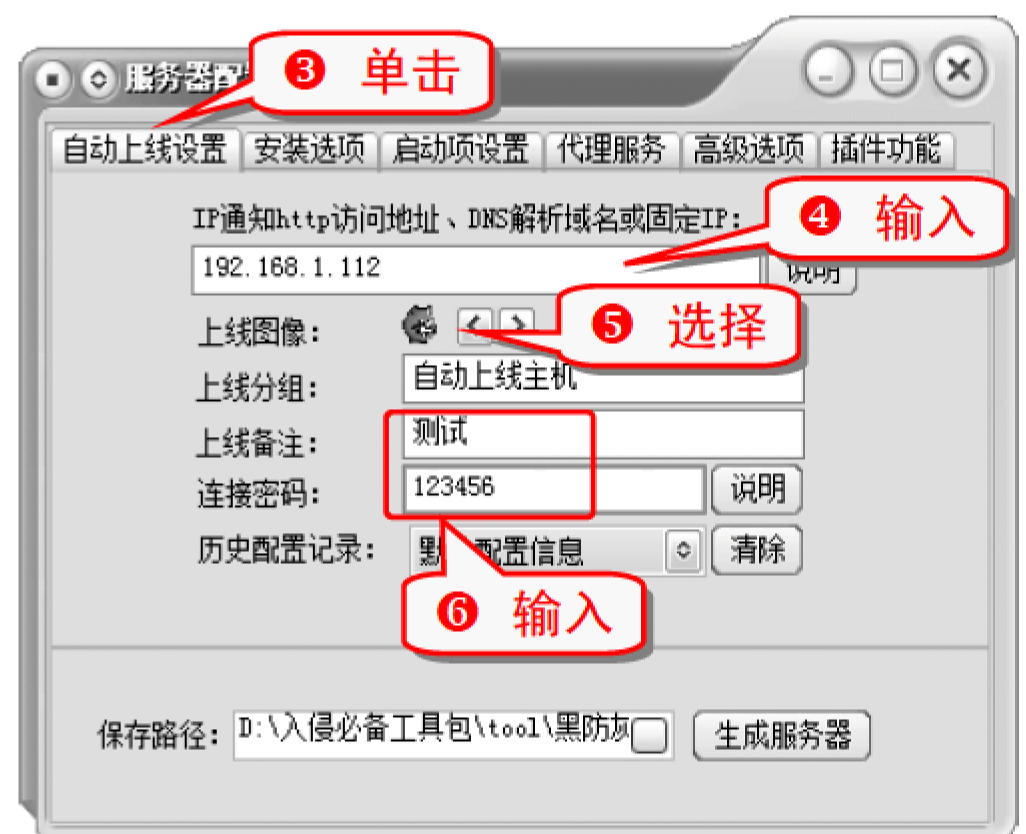
灰鸽子分为客户端和服务端两个部分，客户端是控制者，服务端是受控者(木马)，服务端由客户端生成。

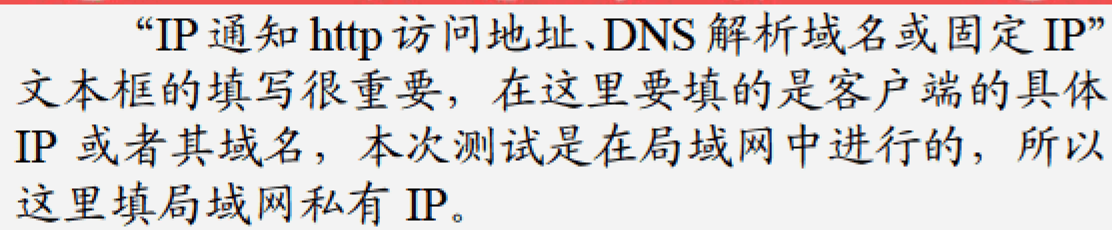
(1) 设置自动上线

服务端主动连接客户端功能是灰鸽子的技术核心，在配置服务端的时候要设置服务端自动上线。

❶ 关闭杀毒软件，运行灰鸽子客户端程序。





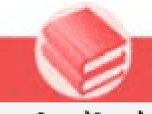


“IP通知http访问地址、DNS解析域名或固定IP”文本框的填写很重要，在这里要填的是客户端的具体IP或者其域名，本次测试是在局域网中进行的，所以这里填局域网私有IP。

专　家　坐　堂

公网IP：经过注册的，在世界各地能够表示唯一位置的，而且可以通过路由查到的IP地址。

私有IP：没有被注册过的，但是可以访问外网，而外网不能直接访问的IP地址。



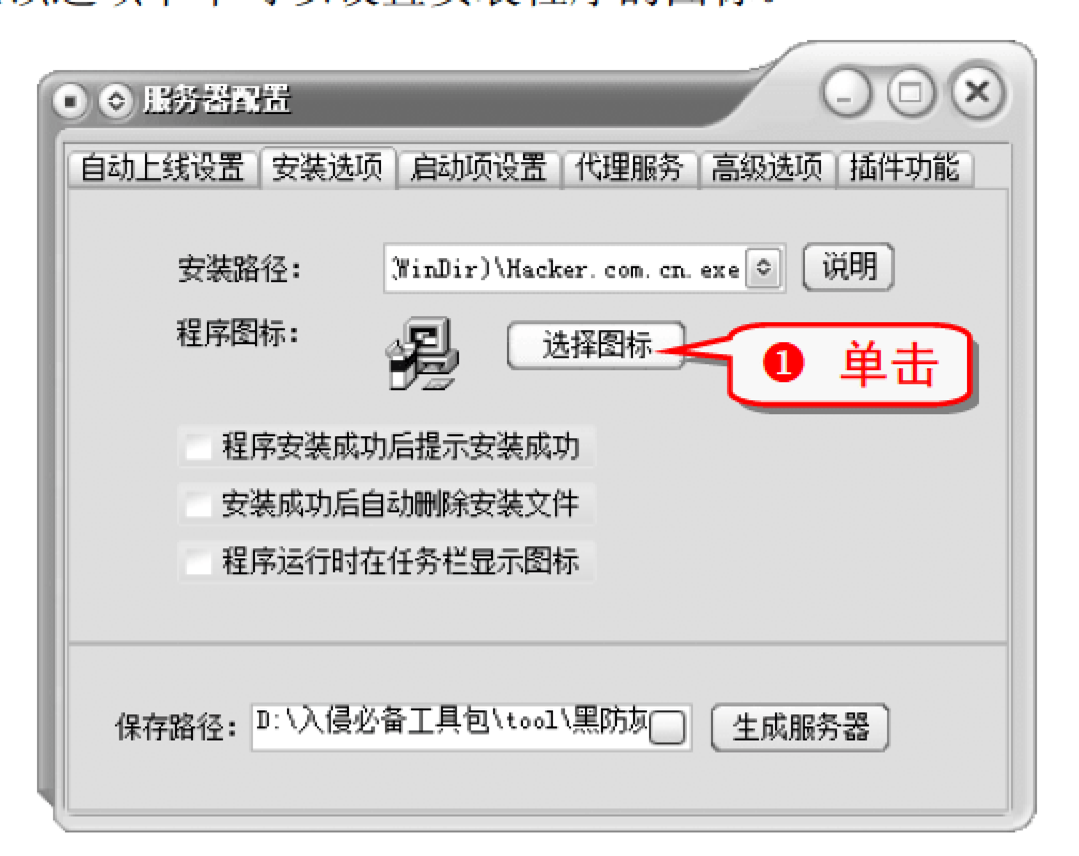
举　一　反　三

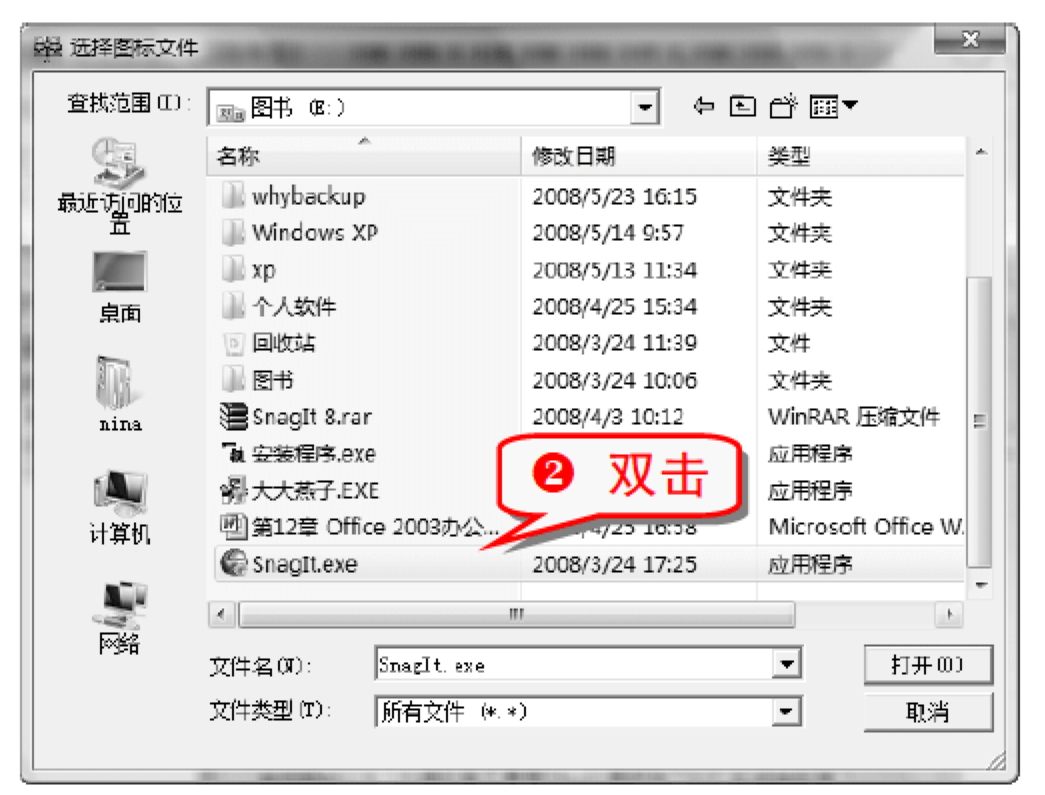
目前ADSL用户基本上都采用动态IP接入方式连接到互联网上。

如果不是在局域网内进行测试，则必须使用动态域名，绑定该动态IP，然后在“IP通知http访问地址、DNS解析域名或固定IP”文本框中填入动态域名，这样服务端才能连接到客户端。

(2) 设置安装选项

单击“安装选项”选项卡可以进入服务端安装的设置，在该选项卡中可以设置安装程序的图标。



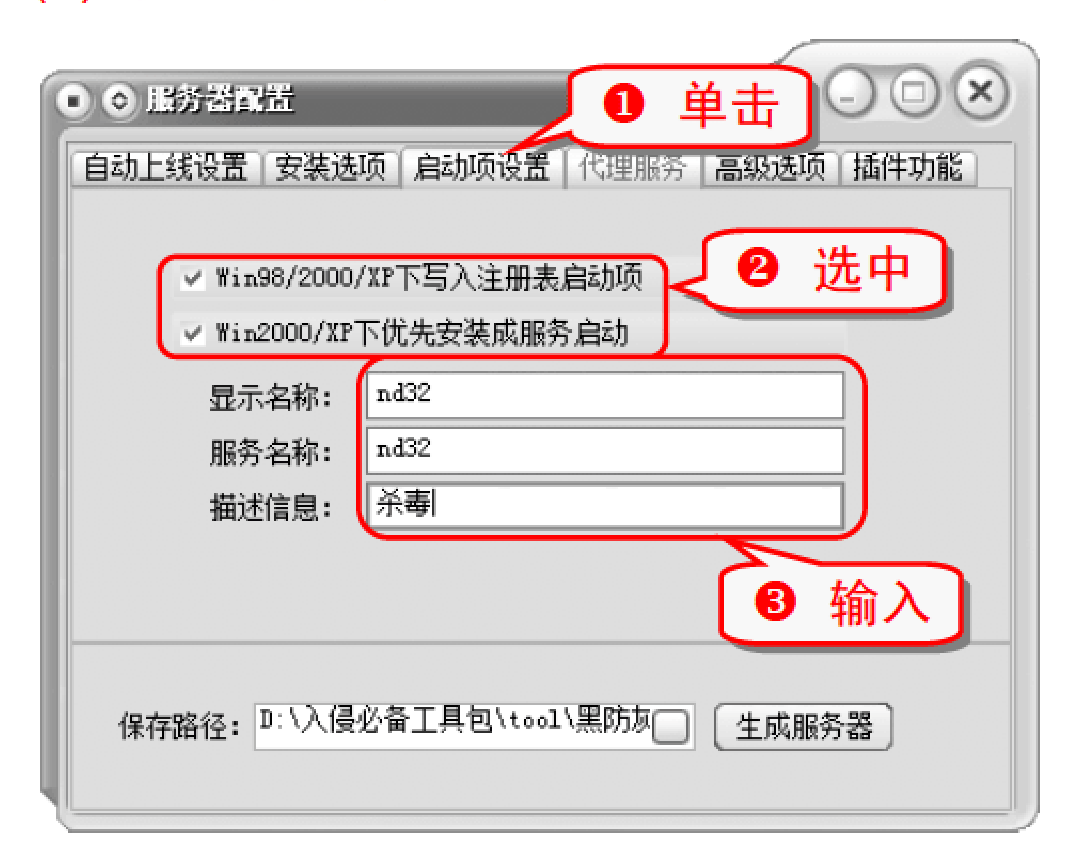




注 意 事 项

安装图标选择得好，会起到很好的迷惑作用，让被控主机自愿运行该服务端程序，从而达到激活木马的目的。

(3) 设置启动项



知 识 补 充

选中“Win98/200/XP 下写入注册表启动项”和“Win200/XP 下优先安装成服务启动”复选框，则被控端主机在每次开机后会自动激活木马程序。

举 一 反 三

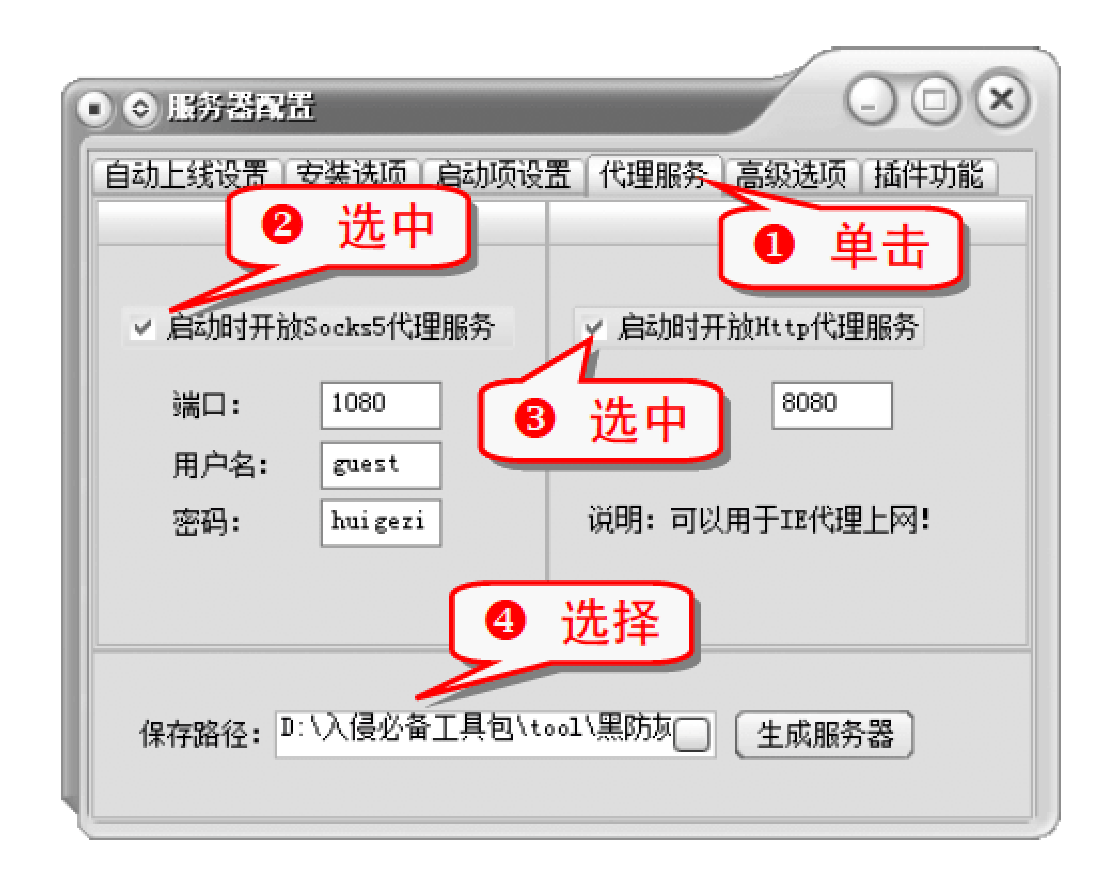
选项卡中的“显示名称”、“服务名称”和“描述信息”文本框可以由自己填写，一般都会填一些类似系统服务的信息去迷惑人。

下图是中了灰鸽子的被控主机的启动项服务，其中的 nd32 就是通过启动项设置伪装的。



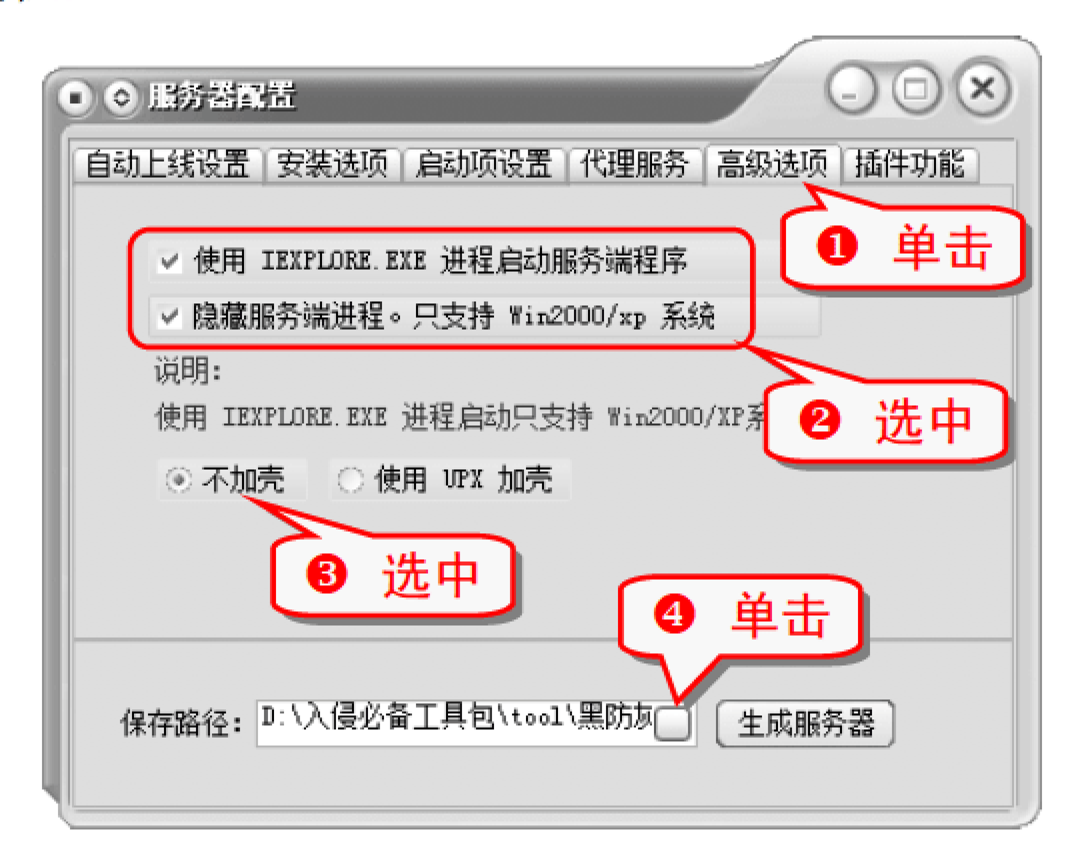
(4) 设置代理服务器

设置代理服务器起的是“借刀杀人”的效果，利用被控的“肉鸡”对别的电脑进行攻击。



(5) 设置高级选项以及生成服务端

任务管理器中可以显示出所有的进程，用户能够通过任务管理器查看可疑进程，而灰鸽子木马可以隐藏主机的进程。









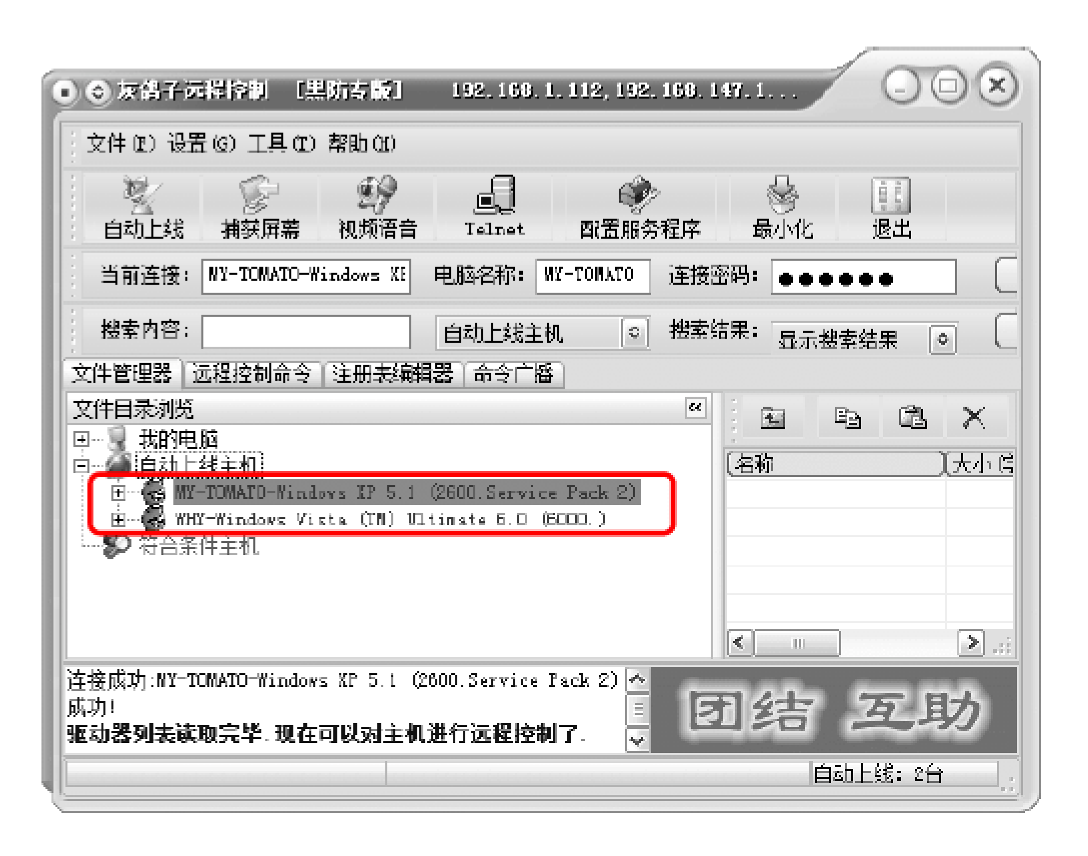




(6) 远程入侵被控电脑

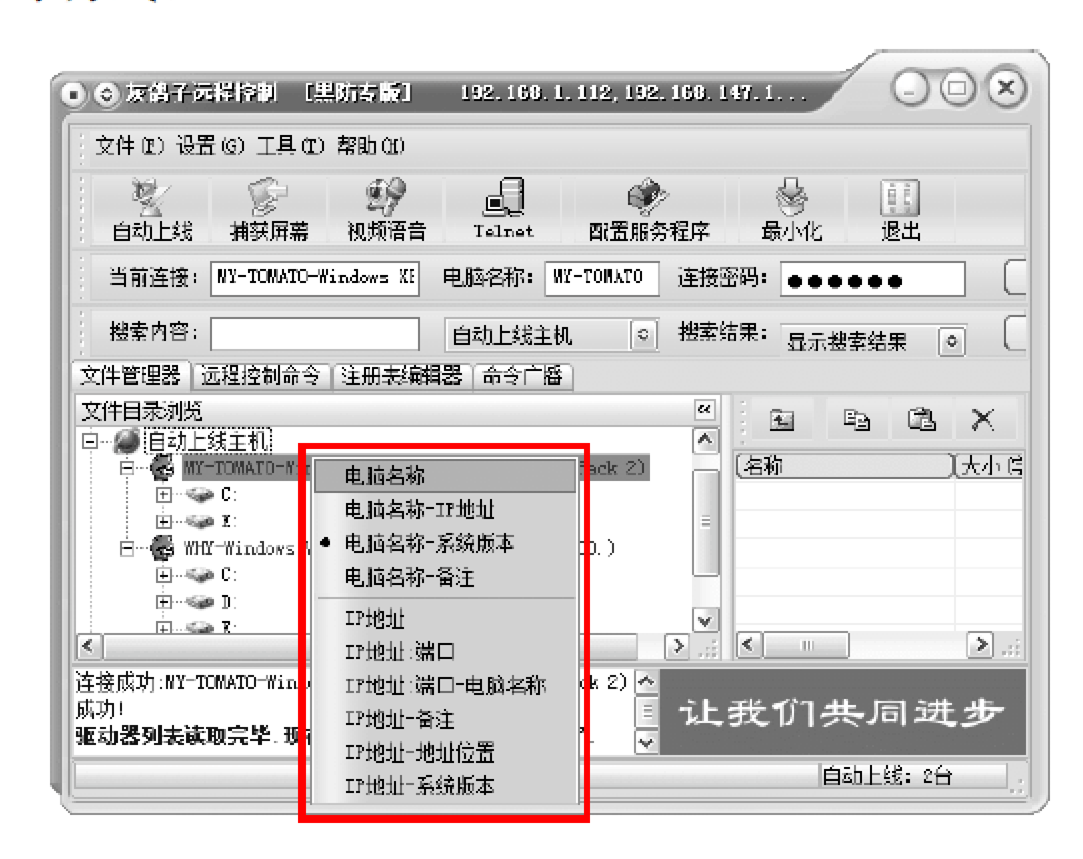
完成服务端的配置以后，当有电脑运行该服务端，服务端会自动寻找对应的客户端，并连接上。

现在将服务端发送到两台电脑上，一台是 Windows Vista 的系统，一台是 Windows XP 的系统。当两台电脑都运行了灰鸽子的服务端后可以发现在“自动上线主机”目录下面多了两台上线主机。

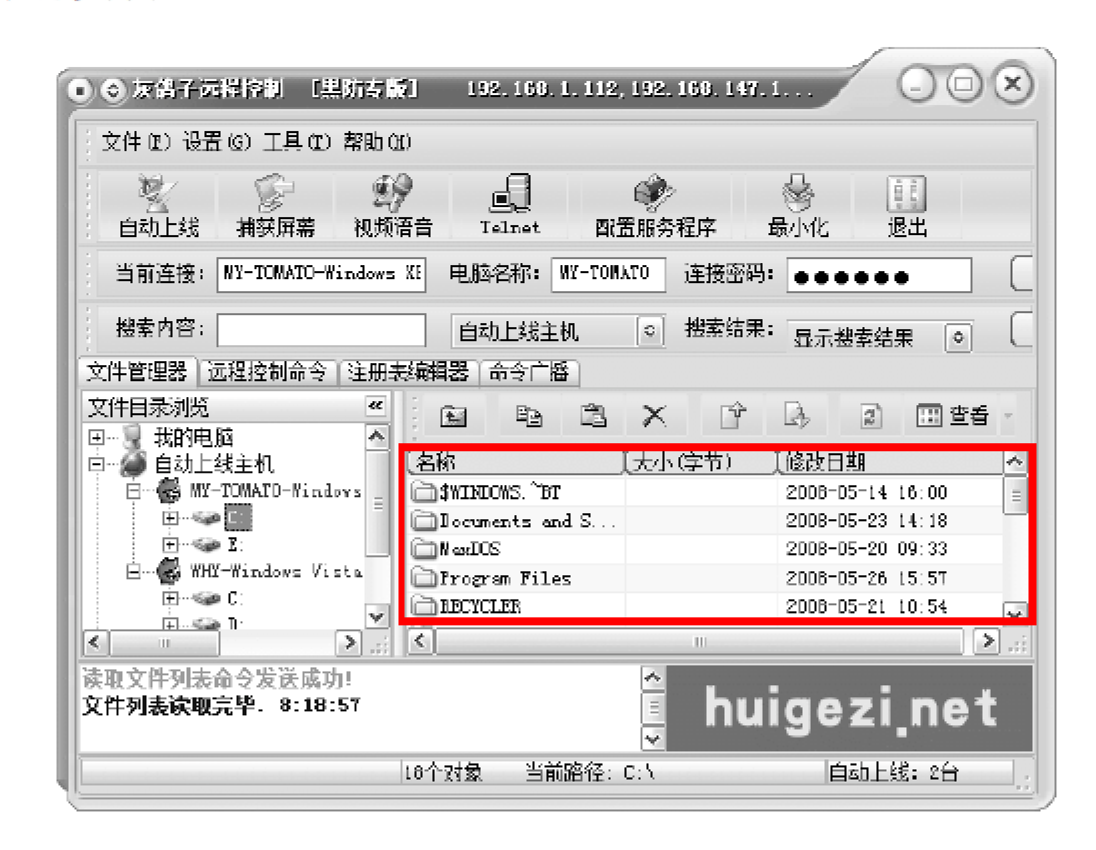


灰鸽子的远程控制能力很强，一旦电脑被控制，就能通过服务端对被控制的电脑做任何事情。

右击被控制主机的名称，在弹出的快捷菜单中可以选择上线主机以什么方式显示。灰鸽子提供了 10 种不同的显示方式。



单击被控主机的盘符，就可以随意查看被控主机上所有的资料。



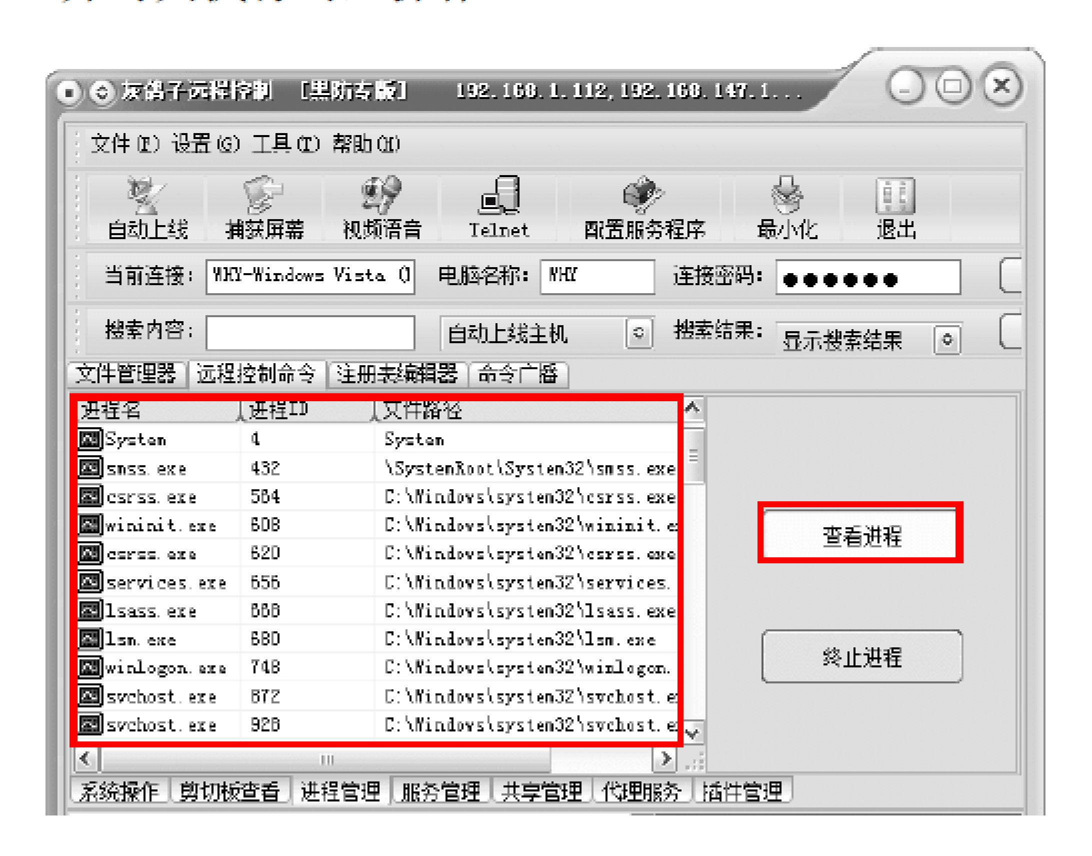
单击“远程控制命令”，选择“系统操作”选项卡，其中有四个按钮，分别是“系统信息”、“重启计算机”、“关闭计算机”和“卸载服务端”。



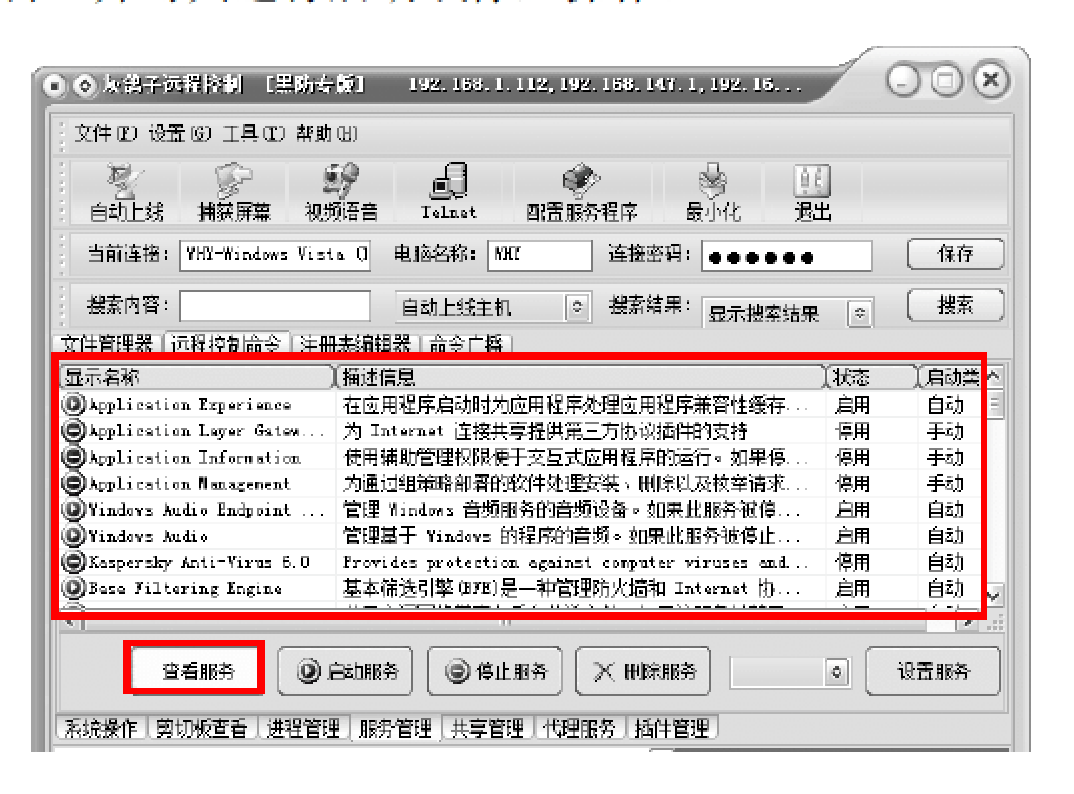
知 识 补 充

“系统信息”：查看远程电脑的详细系统信息。
“重启计算机”：对远程电脑进行远程重启操作。
“关闭计算机”：对远程电脑进行远程关闭操作。
“卸载服务端”：将服务端卸载掉。

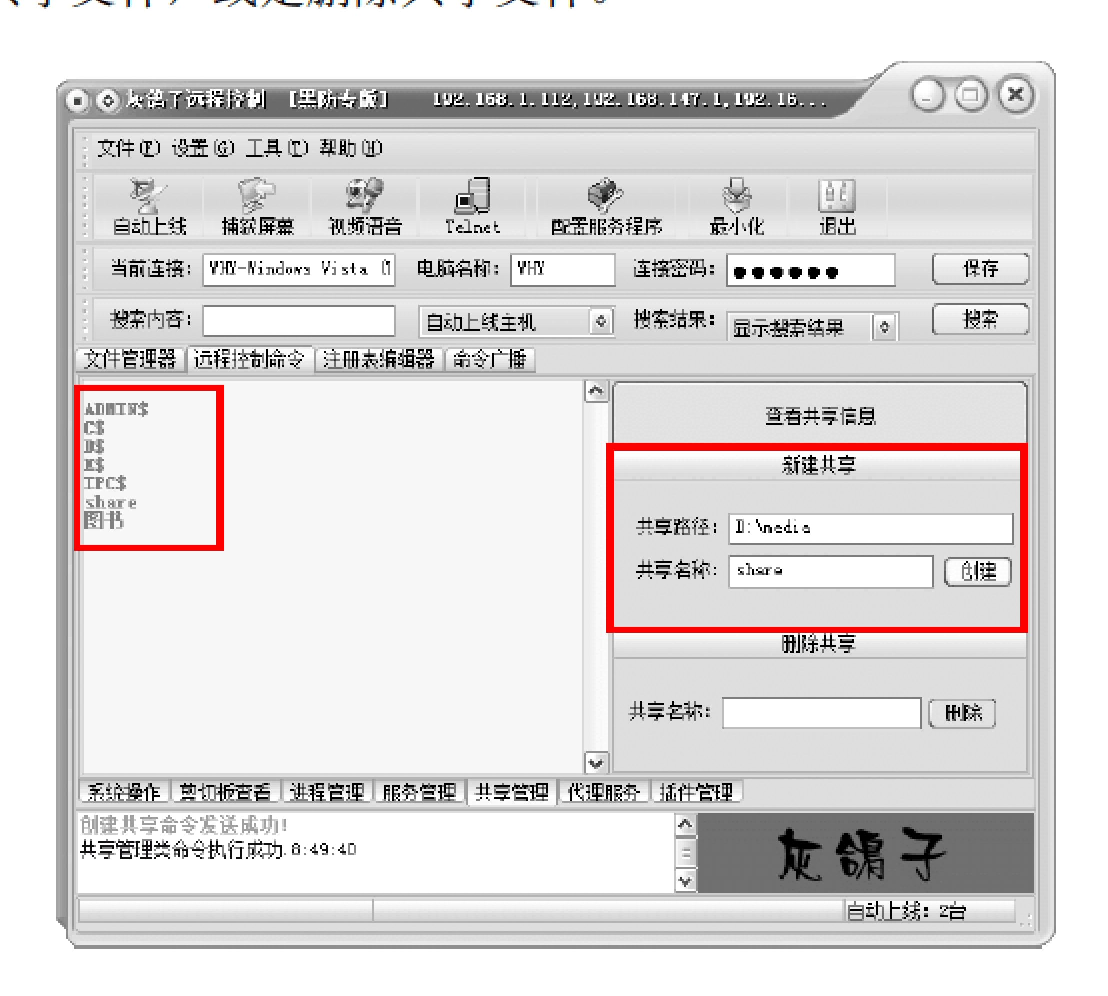
“进程管理”选项卡中可以查看远程电脑的所有进程，并对其执行终止操作。



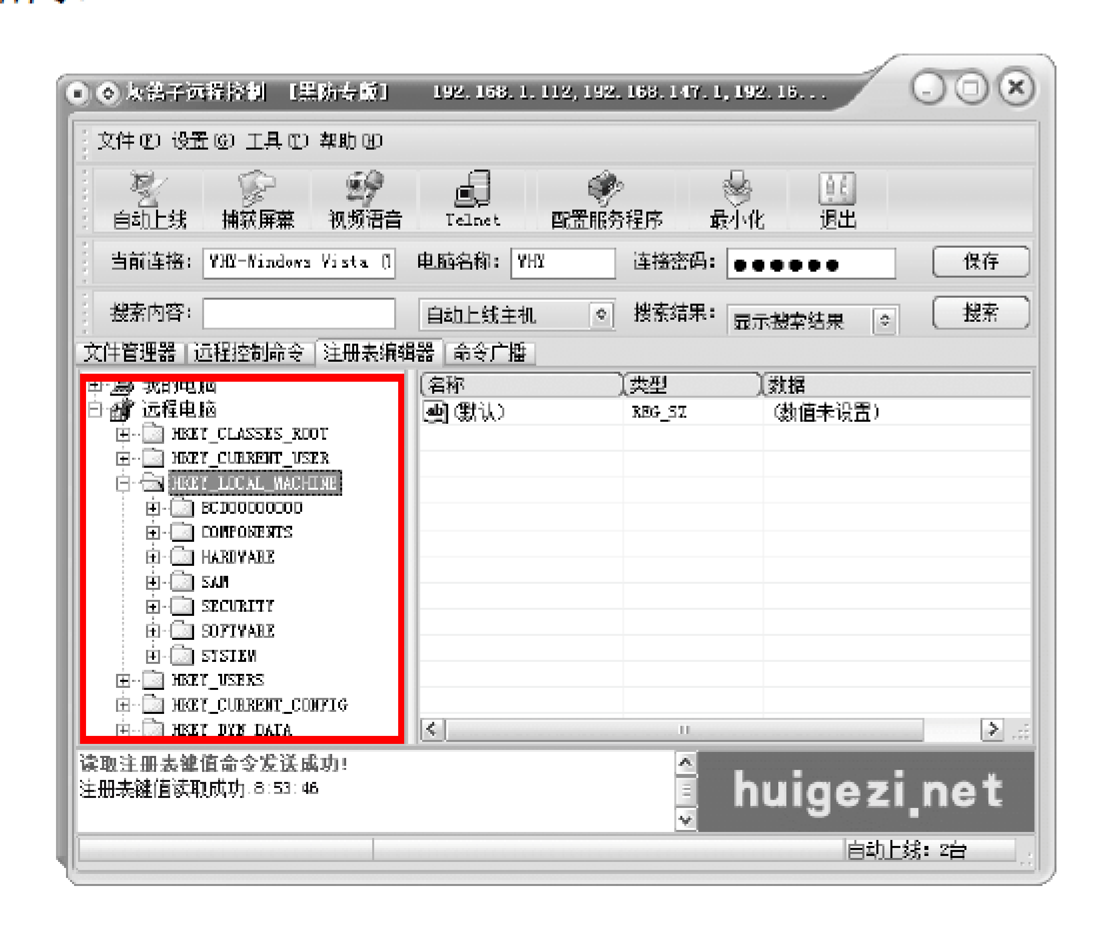
“服务管理”选项卡中可以查看远程电脑所有的服务项目，并对其进行启动或停止操作。



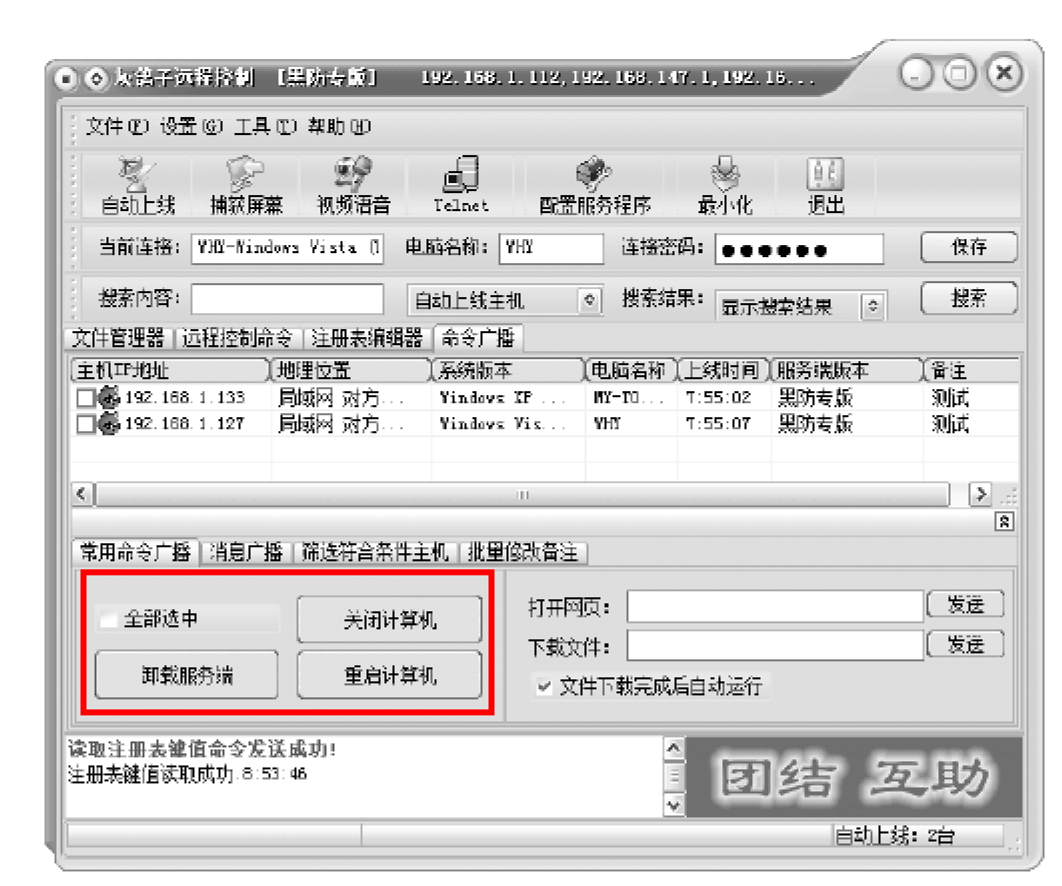
“共享管理”选项卡中可以在远程电脑上创建任意的共享文件，或是删除共享文件。



单击“注册表编辑器”选项卡，可以任意修改远程电脑的注册表编辑器，与在远程电脑上运行注册表编辑器相同。



单击“命令广播”选项卡，可对远程电脑执行“关闭计算机”、“重启计算机”以及“卸载服务端”等操作。





单击工具栏上的“抓获屏幕”按钮，可以打开远程电脑的桌面窗口。





远程屏幕窗口上有工具栏。

- 的作用是控制远程电脑的鼠标和键盘。
- 的作用是让远程屏幕变成全屏模式。
- 的作用是保存远程屏幕，保存符号旁边有一个下拉按钮，单击弹出一个下拉菜单，选择远程屏幕的保存形式。

保存当前画面
录制为MPEG文件

- 发送组合键 旁边也有一个下拉菜单，选择要发送到远程电脑的组合键。发送组合键的作用相当于在远程电脑按下所发送的组合键。



单击工具栏上的“视频语言”按钮，可以打开远程电脑的视频并录制对方的语音聊天。



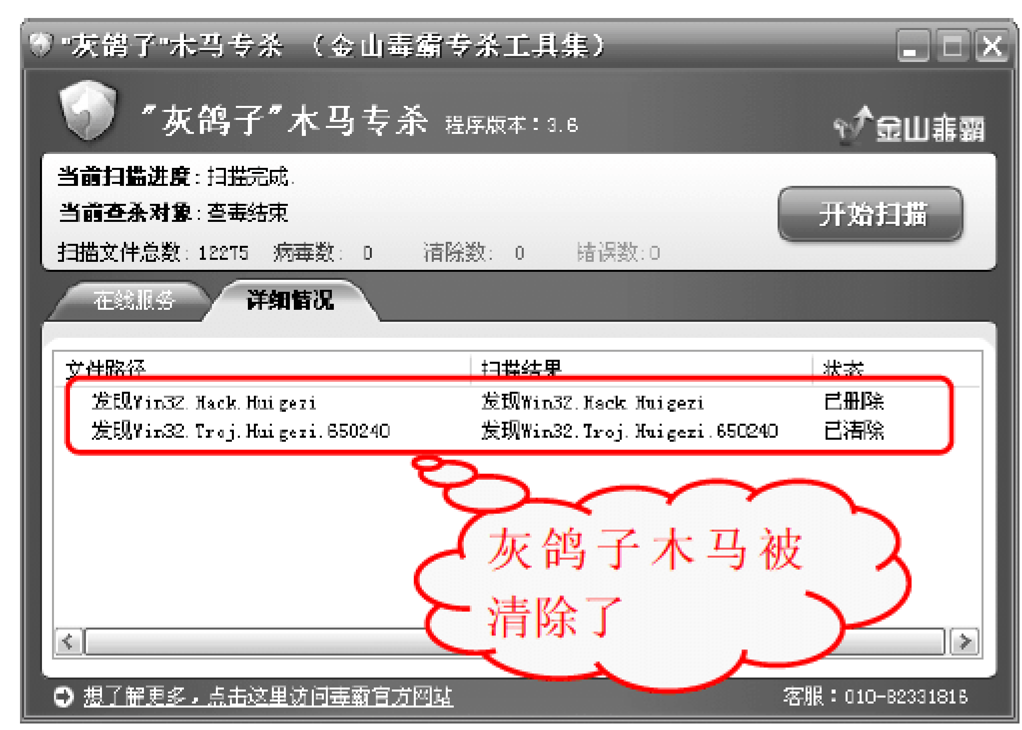
由此可见灰鸽子作为远程控制软件是非常优秀的，但作为远程监控木马，危害却是非常大的。

技巧309　巧用专杀工具清除灰鸽子木马

现在网络上有很多的灰鸽子木马专杀工具，可以快速清除系统中的灰鸽子木马，这里介绍一款金山毒霸的灰鸽子木马专杀工具，可以快速有效地查杀灰鸽子木马。

❶ 从网上下载金山毒霸的“灰鸽子”木马专杀，双击运行。





技巧310 Byshell 木马程序

Byshell 是一个无进程、无 DLL、无启动项的，集多种 Rootkit 技术特征的独立功能远程控制后门程序(Backdoor)，是内核级的木马程序，有很强的隐蔽性和破坏力。

当 Byshell 被安装在一台远程电脑上后，黑客就拥有完全控制该机器的能力，并且很难被已控制电脑所安装的杀毒和防火墙等软件及管理员手工检测出来。

(1) 配置服务端

❶ 运行 Byshell 可执行文件。



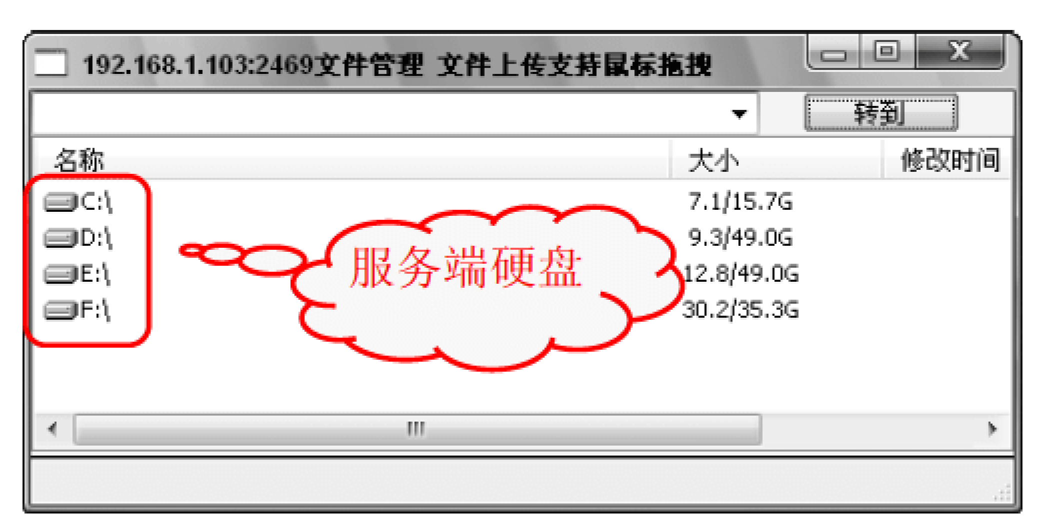


(2) 进行远程监控

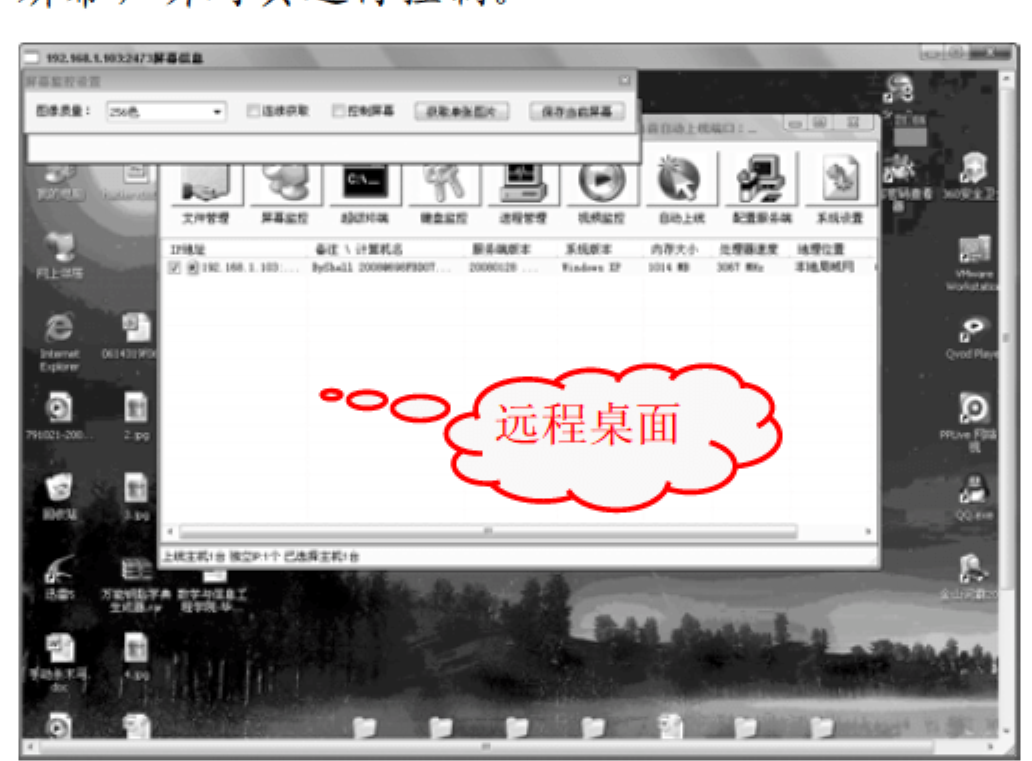
服务端配置成功以后生成一个 Server.exe 的文件，双击运行后自动删除安装文件。

❶ 在远程电脑上双击运行服务端，在主控端上出现一个上线 IP。

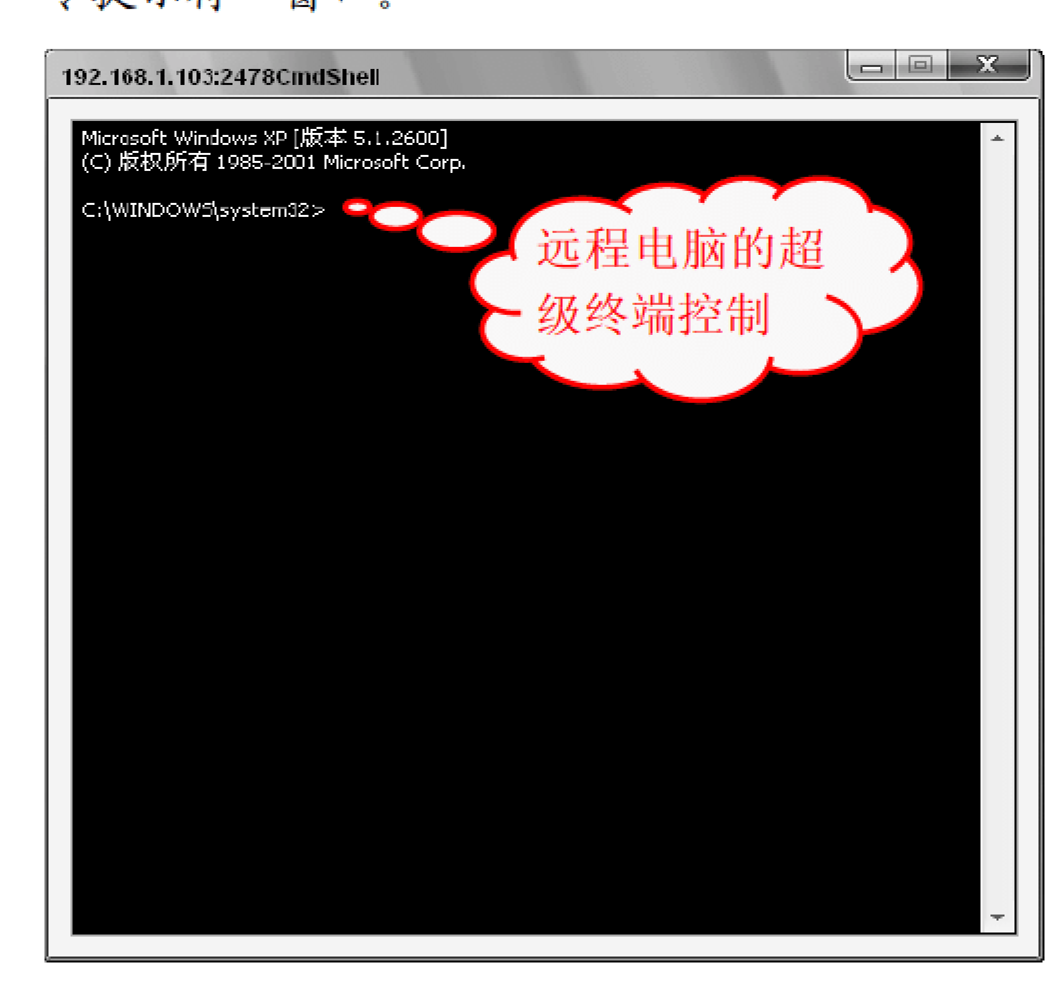




❹ 单击“屏幕控制”按钮，打开远程服务端电脑的桌面屏幕，并对其进行控制。

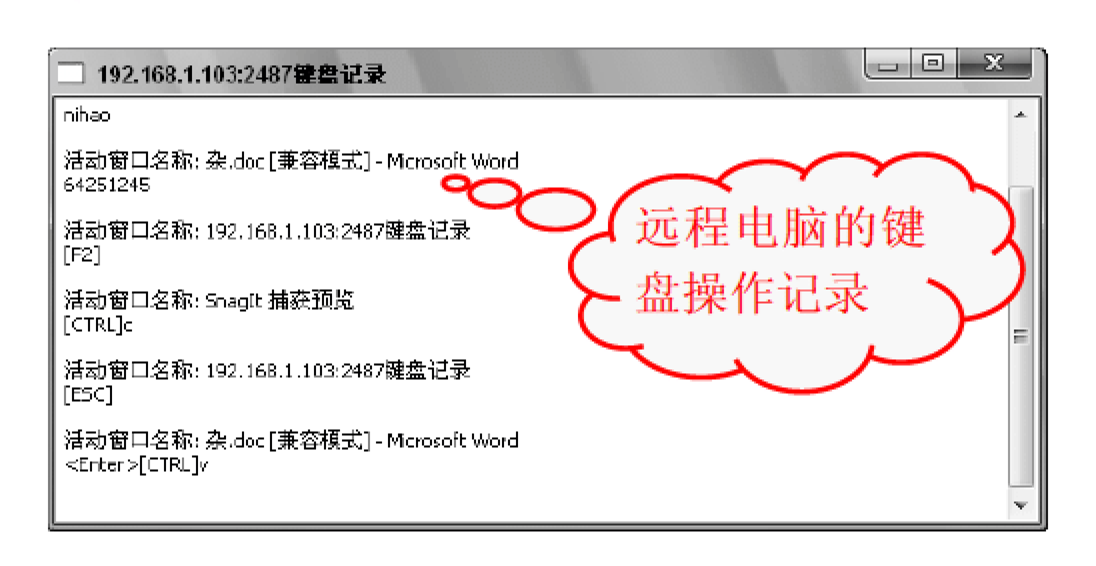


❺ 单击“超级终端”按钮，相当于打开远程电脑的“命令提示符”窗口。





❻ 单击“键盘监控”按钮，打开对远程电脑的键盘记录窗口。

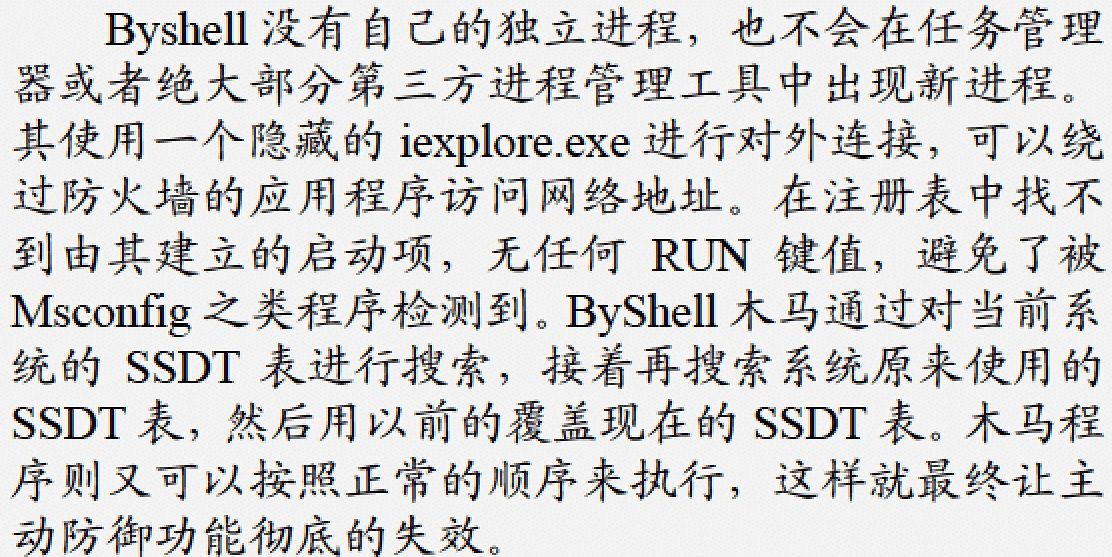


❼ 单击“进程管理”按钮，打开对远程电脑的进程管理窗口。



❽ 单击“进程管理”按钮，打开对远程电脑的进程管理窗口。





知 识 补 充

Byshell 没有自己的独立进程，也不会在任务管理器或者绝大部分第三方进程管理工具中出现新进程。其使用一个隐藏的 iexplore.exe 进行对外连接，可以绕过防火墙的应用程序访问网络地址。在注册表中找不到由其建立的启动项，无任何 RUN 键值，避免了被 Msconfig 之类程序检测到。ByShell 木马通过对当前系统的 SSDT 表进行搜索，接着再搜索系统原来使用的 SSDT 表，然后用以前的覆盖现在的 SSDT 表。木马程序则又可以按照正常的顺序来执行，这样就最终让主动防御功能彻底的失效。

技巧311　巧用木马杀客

木马杀客又名木马清道夫，是专门的反木马工具，软件采用杀毒引擎辨别特征码和传统病毒库辨别方式，可查杀密码偷窃类木马、QQ 尾巴类木马、冰河类木马、网游盗号类木马、灰鸽子类木马以及各种未知木马和黑客程序等。木马内置内存监控及注册表监控功能，木马感染内存及修改注册表启动等都将被监控查杀。其主界面如下图所示。



木马杀客有 9 个功能模块，是一款非常强大的木马清除工具，下面介绍扫描进程、扫描硬盘、扫描注册表三个模块的操作步骤。

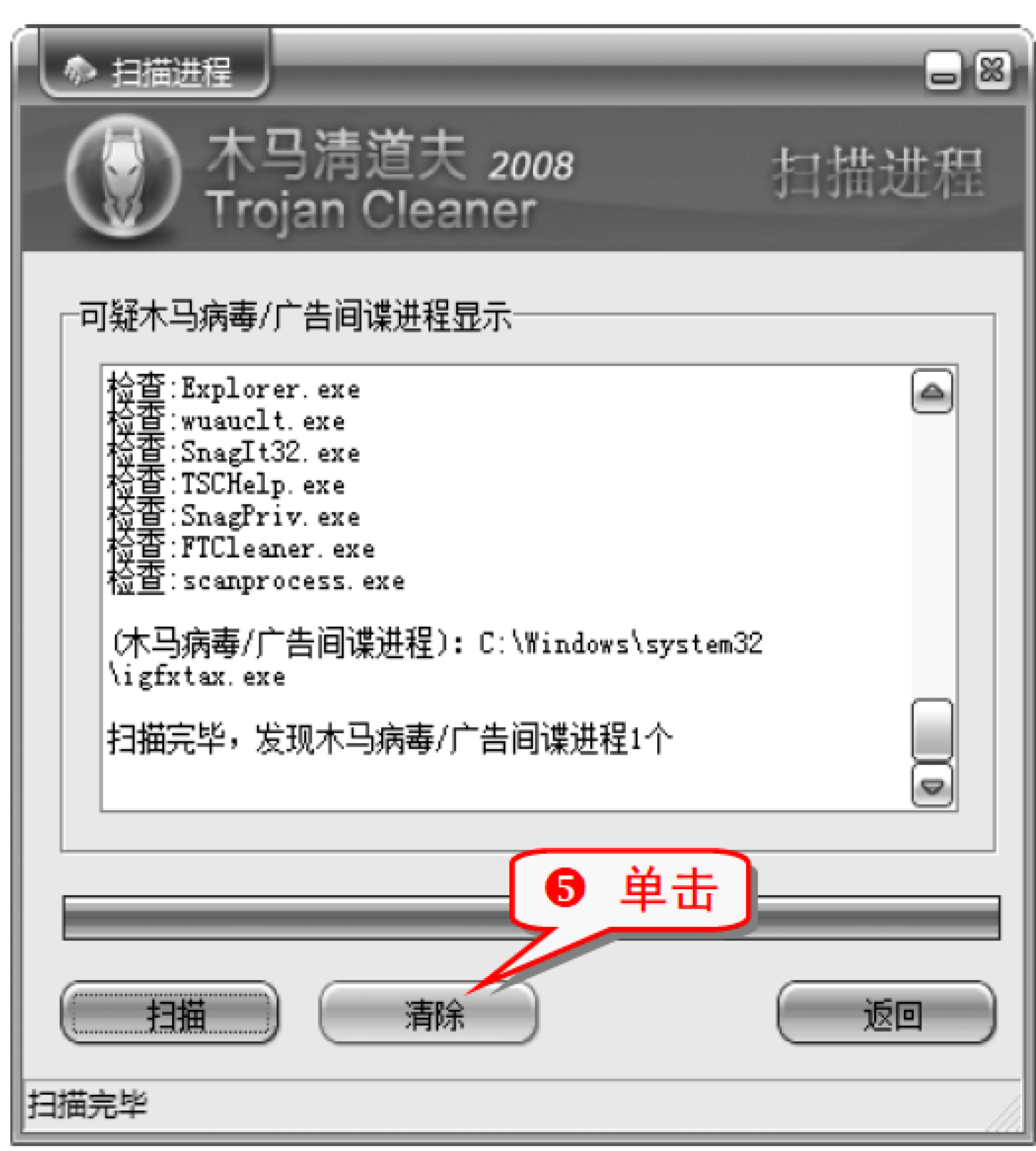
(1) 扫描进程

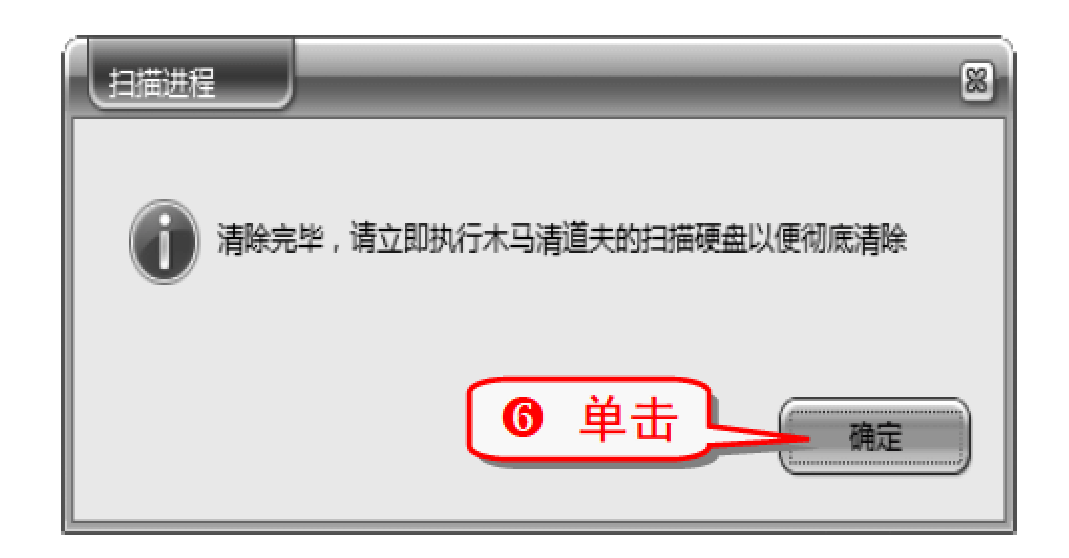
❶ 安装完木马杀客后，运行主程序。











(2) 扫描硬盘

为了能彻底清除木马，有必要对硬盘进行扫描。














专 家 坐 堂

扫描硬盘采用三种引擎扫描方式。

高速扫描硬盘(文件定位引擎)，快速扫描系统已经感染的木马病毒。

精确扫描硬盘(特征码扫描引擎)，对指定驱动器、目录和文件进行扫描，判断是否有木马病毒。

NTFS 数据流扫描，专门针对 NTFS 磁盘文件格式的数据流扫描技术，对未知隐藏的可疑数据进行清除。

(3) 扫描注册表

扫描注册表的错误和被恶意修改的项目。











技巧312　手动查杀系统中的隐藏木马

使用木马查杀软件可以清除大多数木马程序，但对于极少数软件不能识别的木马程序，只有通过手动进行查杀。

(1) 用 msconfig 命名禁止木马程序启动

msconfig 是 Windows 操作系统内置的系统配置实用程序，通过该程序可以配置系统的启动项目和系统服务，在 Windows Vista 系统中使用该命令可以对“常规”、“启动”、“服务”、“启用”以及“工具”五部分进行配置，对于已知的木马程序，用户可通过 msconfig 将其禁止启动，重新启动后再进行手工删除。

❶ 打开“运行”对话框，输入 msconfig 命令，按下 Enter 键，打开“系统配置”对话框。



 举 一 反 三 

对于可疑的服务，都可以在这里将其禁止。

(2) 检查注册表的可疑键值

有些木马会在注册表中的启动项加入自身键值，以达到开机运行的目的，此时用户可对注册表的相应键值进行检测，如果发现有可疑项目，直接将其删除即可，需要注意的是，在操作注册表时一定要谨慎，在无法确定其是否为木马时，最好不要直接进行操作，在对注册表操作前，一定要做好备份，以备在需要时，恢复注册表。

用户一般可检查如下键值，如发现有木马项目存在，直接将其删除并重新启动电脑即可。

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

HKEY_CURRENT_USER/Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

HKEY_CURRENT_USER/Software\Microsoft/Windows\CurrentVersion/Explorer/ShellFolders

(3) 检查系统安装目录下的可疑文件

木马在服务端运行之后，会在电脑的系统目录下产生一个安装文件，用户可以通过查找系统目录下的可疑文件，将其删除，这样也能达到查杀的效果。

❶ 将系统隐藏的文件显示出来。

❷ 查找带有可疑后缀名的文件，如 com.cn.exe 或者 hacker.exe。

❸ 将其彻底删除。

(4) 检查 WIN.INI 和 SYSTEM.INI 文件

- 在 WIN.INI 文件中，通常以 run=和 load=字段载入执行的应用程序，如果这两个字段下有可疑项，可将其删除。
- 在 SYSTEM.INI 文件中，通常会以“shell=文件名”的方式加载应用程序，如果在文件中存在可疑的加载选项，可将其删除。

(5) 使用 DOS 命令

使用 DOS 命令，可以快捷地检查当前运行的进程中，是否有木马程序，并可以通过命令将其关闭。

在 DOS 命令行下，输入如下命令：

```
tasklist /svc
```

此时会显示当前运行的所有进程名和其相对应的服务，如果某个进程与可疑服务进行了关联，则很可能是木马程序。

在 DOS 命令行下，输入如下命令：

```
netstat –an
```

此时会显示所有主机与外界建立连接的端口和端口状态，如果发现其中某一端口与陌生的 IP 地址发生了联系，则系统很可能中了木马病毒。

对于可疑的进程，可使用 DOS 命令将其立即关闭，在 DOS 命令行下，输入如下命令：

```
ntsd -c q -p PID
```

其中 PID 选项为可疑进程的进程号，此命令可强制关闭指定的进程。

技巧313 360 顽固木马专杀大全

360 顽固木马专杀大全提供“一站式”解决木马方法，最快最全地解决系统诸多的问题。

(1) 查杀木马

❶ 打开 360 顽固木马专杀大全主窗口。

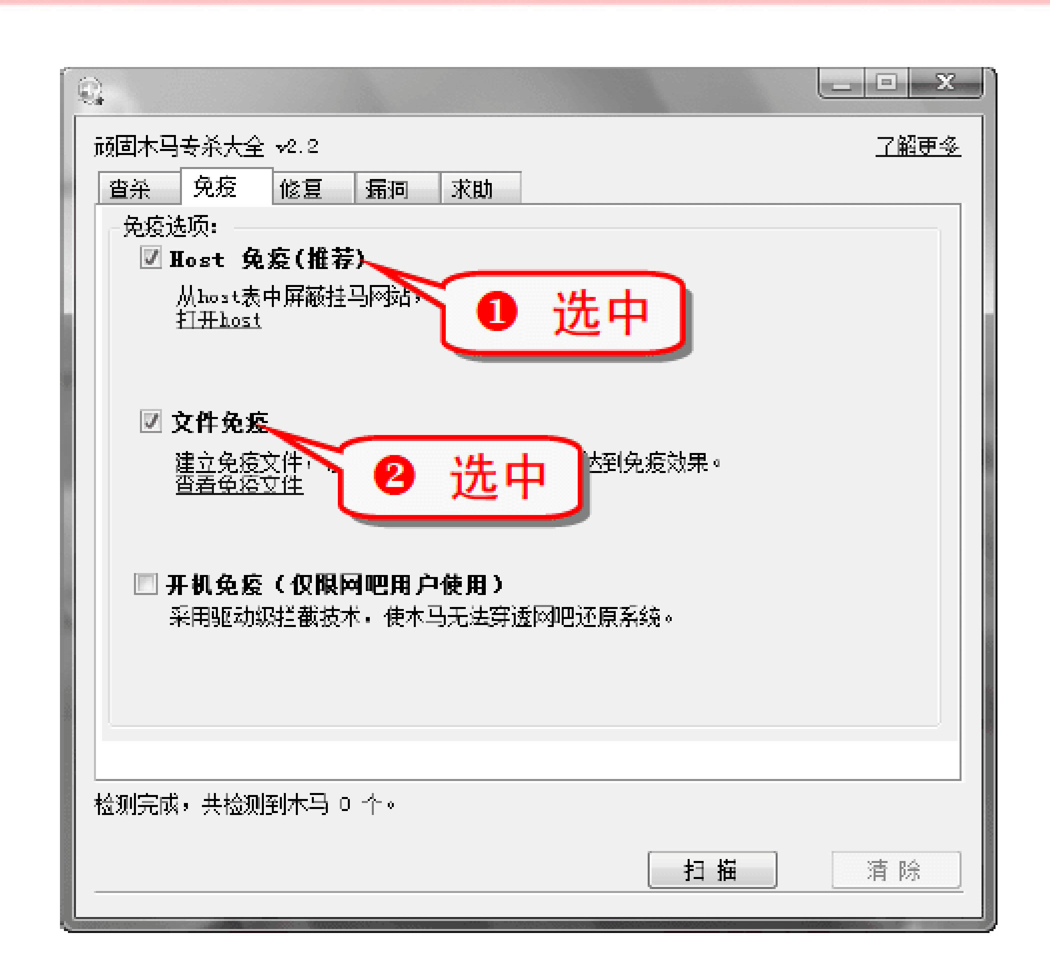


(2) Host 免疫以及文件免疫

hosts 文件是 Windows 系统中一个负责 IP 地址与域名快递解析的文件，以 ASCLL 格式保存。电脑在键入域名的时候，首先会去看看 hosts 文件汇总有没有关于此域名 IP 地址的记录，如果有，就直接登录该网站。

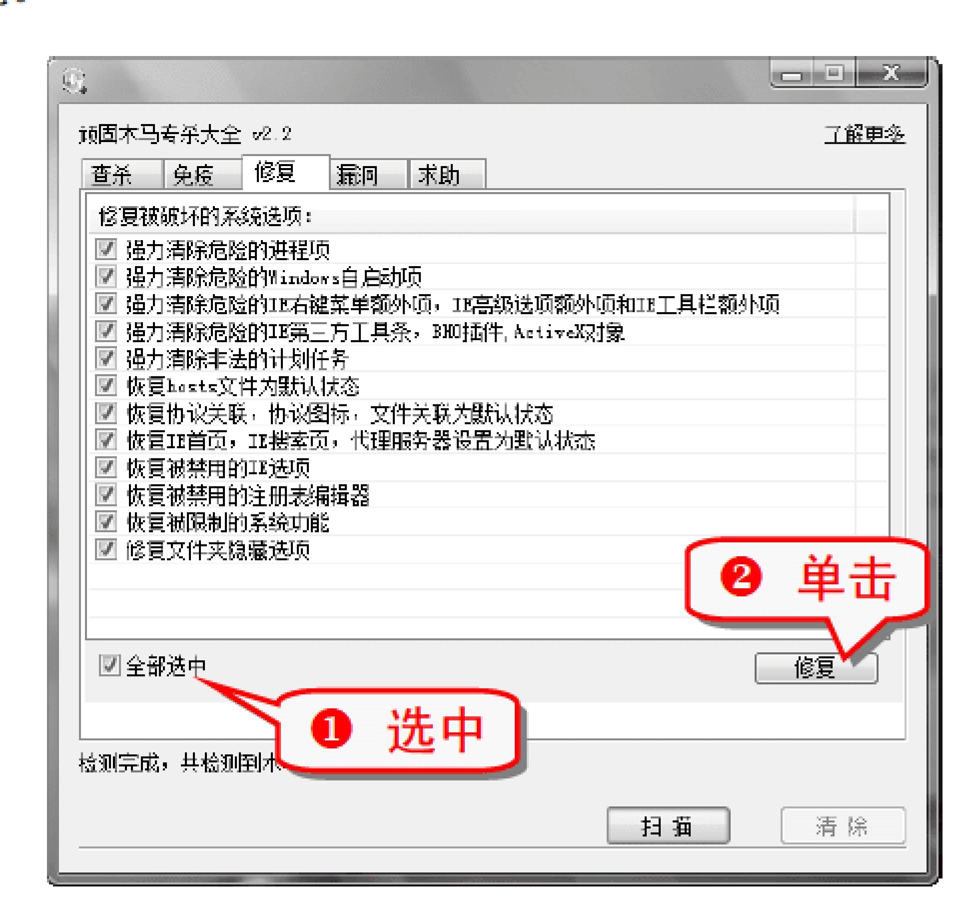
Host 免疫就是利用 host 表的这一功能，将一些木马下载源头网站进行屏蔽，即使不小心点击到这类网站也不会正常访问，从而达到切断木马源头的效果。

文件免疫就是创建一些与木马文件同名的 0KB 大小文件夹，采用驱动级保护，使木马文件无法创建成功，从而达到免疫木马的目的。



(3) 修复被破坏的系统选项

360 顽固木马专杀大全提供了修复被破坏的系统选项功能。

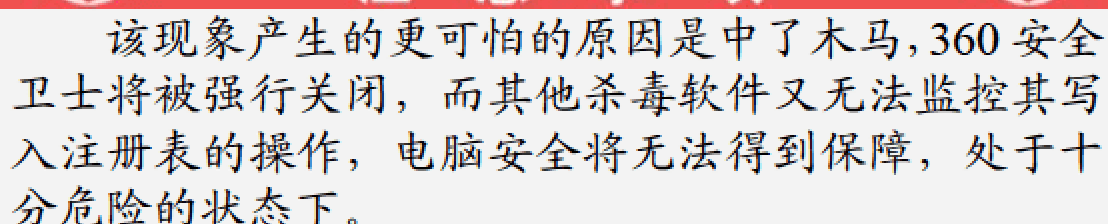


技巧314　44939.com 首页篡改修复工具

浏览器主页被莫名其妙的更改为 www.44939.com（“44939 导航”网站），使用各种 IE 修复工具修复后，在几分钟内没有问题，过一段时间或下次开机以后，主页会再次被修改为 44939 导航。使用 360 的 44939.com 首页篡改修复工具可以解决该问题。

❶ 到 360 安全中心下载 44939.com 首页篡改修复工具，双击运行。





注　意　事　项

该现象产生的更可怕的原因是中了木马，360 安全卫士将被强行关闭，而其他杀毒软件又无法监控其写入注册表的操作，电脑安全将无法得到保障，处于十分危险的状态下。

专　家　坐　堂

电脑有以上症状，请立刻下载 44939 专杀，对电脑进行扫描，如果发现此木马请立刻清除。因为这些木马程序，会盗窃用户隐私、账号密码、虚拟财产和其他数据。

技巧315　判断电脑是否感染了病毒

电脑病毒有“良性”和“恶性”之分。“良性”病毒不会破坏电脑数据，但是会造成系统程序工作异常；“恶性”病毒会破坏电脑数据，甚至破坏电脑的硬件。

通过以下几个症状可以判断电脑是否已中病毒。

(1) 系统出现异常

出现网页、文件打不开或是死机等异常现象。

(2) CPU 占用 100%

打开 Windows 任务管理器，发现 CPU 使用率达到 100%。

(3) Windows 出现异常出错信息

经常弹出警告信息或是出错信息。

(4) 运行速度变慢

系统的运行速度变得非常慢，很久才响应相应的操作。

(5) 内存不足

运行正常的程序时出现内存不足的情况。

(6) 进程变多

打开 Windows 任务管理器，发现进程增加了很多。

举　一　反　三

最行之有效的方法是利用各种正版的杀毒软件来检测电脑是否已中病毒。

技巧316　恶意代码的定义

恶意代码是具有恶意的目的，本身是程序并且通过执行发生作用的代码。

恶意代码具有以下症状。

(1) IE 主页被修改

默认的 IE 主页被改为其他的网页。

(2) 主页设置被锁，且设置选项无效不可更改

主页设置被禁用，主页地址栏变成灰色被屏蔽。

(3) 默认的 IE 搜索引擎被修改

在 IE 浏览器工具栏中有一个搜索引擎的工具按钮，单击这个按钮，即链接到那个篡改网站。

(4) IE 标题栏被添加非法信息

IE 标题栏中出现了很多恶意网站的信息。

(5) 快捷菜单被添加非法网站链接

单击鼠标右键在快捷菜单中会出现英文词组或广告条文。

(6) IE 收藏夹被强行添加非法网站地址链接

通过修改注册表，强行在 IE 收藏夹内自动添加非法网站的链接信息。

(7) 在 IE 工具栏非法添加按钮

工具栏处添加非法按钮。

(8) 锁定地址栏的下拉菜单及其添加文字信息

通过修改注册表，将地址栏的下拉菜单锁定变为灰色。

(9) IE 菜单“查看”下的“源文件”项被禁用

通过修改注册表，将 IE 菜单“查看”下的“源文件”项锁定变为灰色。

技巧317 弹出全屏窗口的恶意网页代码

利用以下代码制作一个恶意网页，当访问该网页时，会立即弹出一个全屏网页窗口。

❶ 新建一个记事本文件，编写如下代码。

```
<html>
<bodyonload="window.open('http://www.sina.com','example1','fullscreen');">
<b>制作弹出全屏窗口的恶意网页举例</b>
</body>
</html>
```

❷ 将记事本保存为.html 的形式。

❸ 以网页打开方式将其打开，最终效果图如下。




注 意 事 项

网页恶意代码具有攻击性，仅供研究使用。

技巧318 弹出被 F11 化窗口的恶意网页代码

利用以下代码制作一个恶意网页，当访问该网页时，会立即弹出一个只带标签栏的全屏网页窗口。

❶ 新建一个记事本文件，编写如下代码。

```
<html>
<body
onload="window.open('http://www.sina.com','example2','channelmode');">
<b>制作弹出被 F11 化全屏窗口的恶意网页举例</b>
</body>
</html>
```

❷ 将记事本保存为.html 的形式。

❸ 以网页方式将其打开，最终效果图如下。





技巧319　弹出带有收藏链接工具栏窗口的恶意网页代码

利用以下代码制作一个恶意网页，当访问该网页时，会立即弹出一个指定大小的网页窗口。

❶ 新建一个记事本文件，编写如下代码。

```
<html>
<body
onload="window.open('http://www.sina.com','example3','
width=300,height=300,directories');">
<b>制作弹出指定大小窗口的恶意网页举例</b>
</body>
</html>
```

❷ 将记事本保存为“.html”的形式。

❸ 以网页方式将其打开，最终效果图如下。



技巧320　360 磁碟机病毒专杀

磁碟机病毒又名 dummycom 病毒，是一种传播迅速，破坏力很强的病毒。



专　家　坐　堂

感染该磁碟机病毒后主要有如下症状：

系统运行缓慢、频繁出现死机、蓝屏以及报错等现象。

进程中出现两个 lsass.exe 和两个 smss.exe，且病毒进程的用户名是当前登录用户名。

杀毒软件被破坏，多种安全软件无法打开，安全站点无法访问。

系统时间被篡改，无法进入安全模式，隐藏文件无法显示。

病毒感染.exe 文件导致其图标发生变化。

会对局域网发起 ARP 攻击，并篡改下载链接为病毒链接。

弹出钓鱼网站。





知　识　补　充

磁碟机病毒的主要传播渠道是：

- U 盘/移动硬盘/数码存储卡。
- 局域网 ARP 攻击。
- 感染文件。
- 恶意网站下载。
- 其他木马下载器下载。

❶ 下载 360 磁碟机病毒专杀，双击其运行软件，弹出运行窗口。



❷ 按下 Enter 键，进行病毒扫描。

技巧321　360 恶意网站屏蔽器

360 恶意网站屏蔽器是专门针对恶意网站进行屏蔽的辅助工具。同时也可以使用该工具快速修改本机 hosts 表，是一款非常方便实用的小工具。



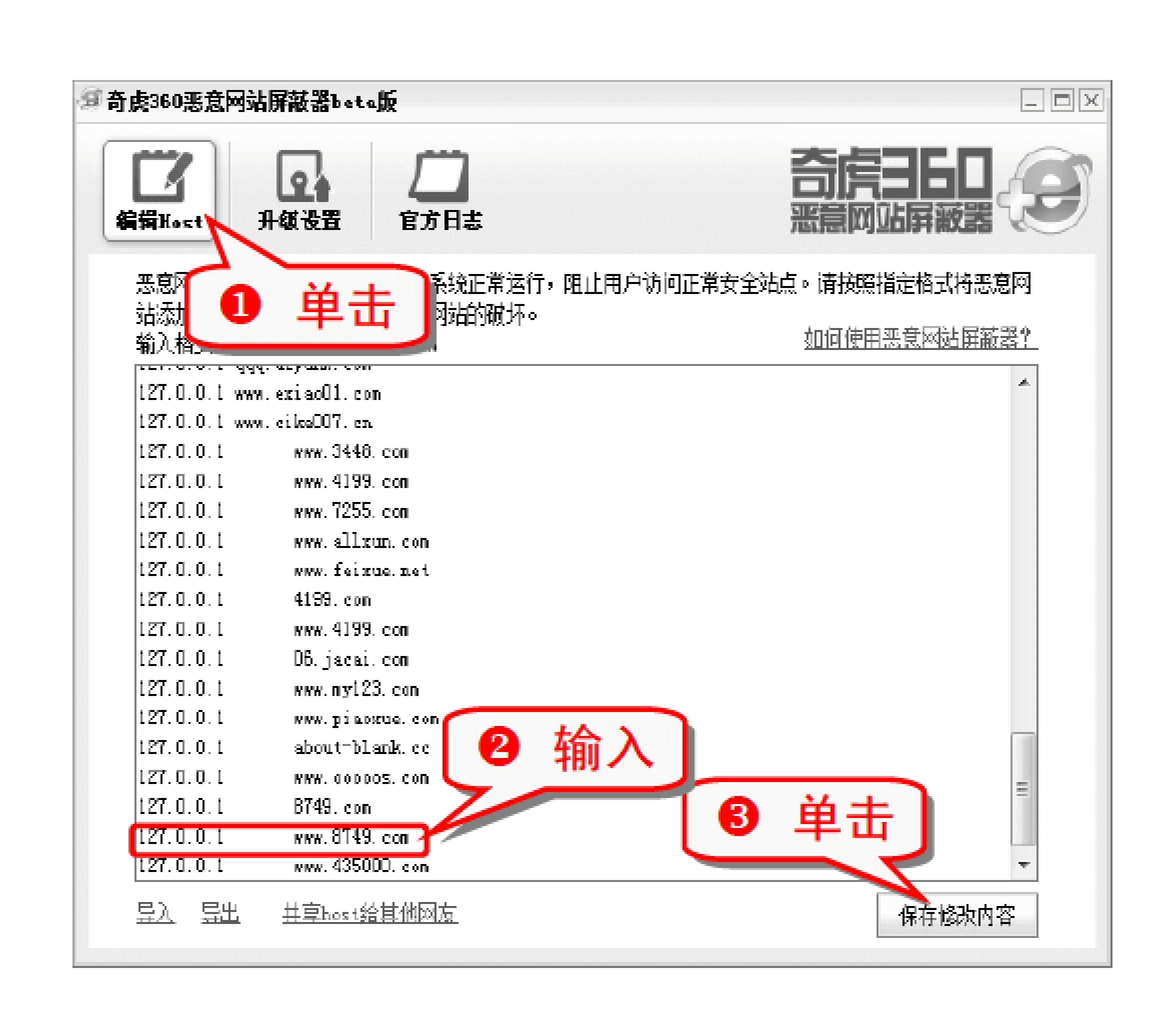
专　家　坐　堂

360 恶意网站屏蔽器主要功能如下：

- 快速编辑 Hosts 表。
- 通过 Hosts 表屏蔽恶意网站。
- 与网友共享 Hosts 表，及时屏蔽最新恶意网站。

(1) 编辑 Host 表

将恶意网站添加进 Hosts 表，格式如：127.0.0.1 www.xxx.com(每行一个)。





举 一 反 三

导入、导出功能可以将本机的 Hosts 表导出成 txt 格式文件，也可以将已编辑好的 txt 格式的 Host 导入覆盖源文件。

共享 Hosts 给其他网友：到 360 百科中共享自己的 Hosts 内容给其他网友。

(2) 升级设置

选中“从官方升级站点自动检测升级”复选框将会在每次启动恶意网站屏蔽器时，检测 360 官方站点是否有新的恶意网站屏蔽 Hosts 发布，如果有更新，将会给出提示。



技巧322 360 U 盘病毒专杀工具

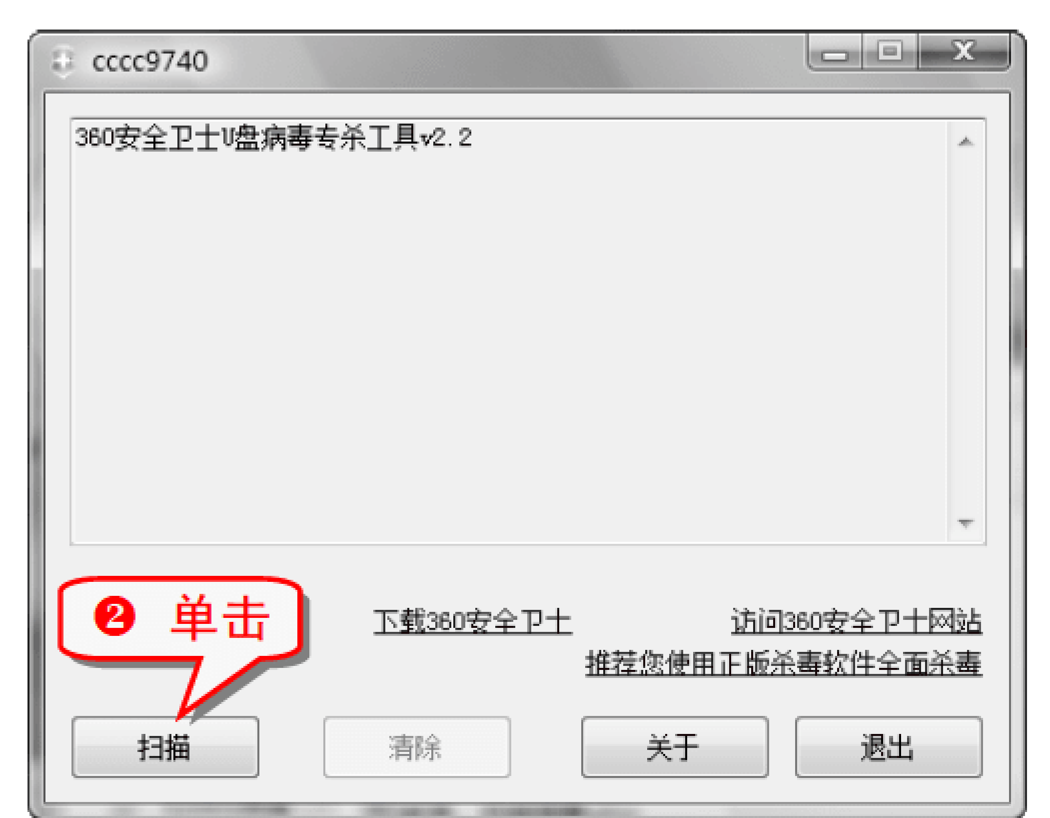
U 盘病毒会在系统中每个磁盘目录下创建 autorun.inf 病毒文件(不是所有的 autorun.inf 都是病毒文件)，因此也被称为“Autorun 病毒”。

知 识 补 充

此类病毒借助“Windows 自动播放”的特性，使用户双击盘符时就可立即激活指定的病毒。另外，此类病毒主要通过 U 盘传播自身，危害极大，不但影响用户的电脑系统，而且可能会造成大规模的病毒扩散等现象。

360 安全卫士 U 盘专杀工具，使用智能启发式查杀方法，对流行的 U 盘病毒及其衍生物具有优秀的灭杀效果。

❶ 下载安全卫士 U 盘专杀工具，双击其运行软件，弹出运行窗口。





专题十二　备份与恢复系统数据

内容导航

无论是病毒还是系统故障都可能造成系统的瘫痪或数据的丢失，因此对系统、驱动程序和注册表进行备份成为日益重要的防范措施。

热点快报



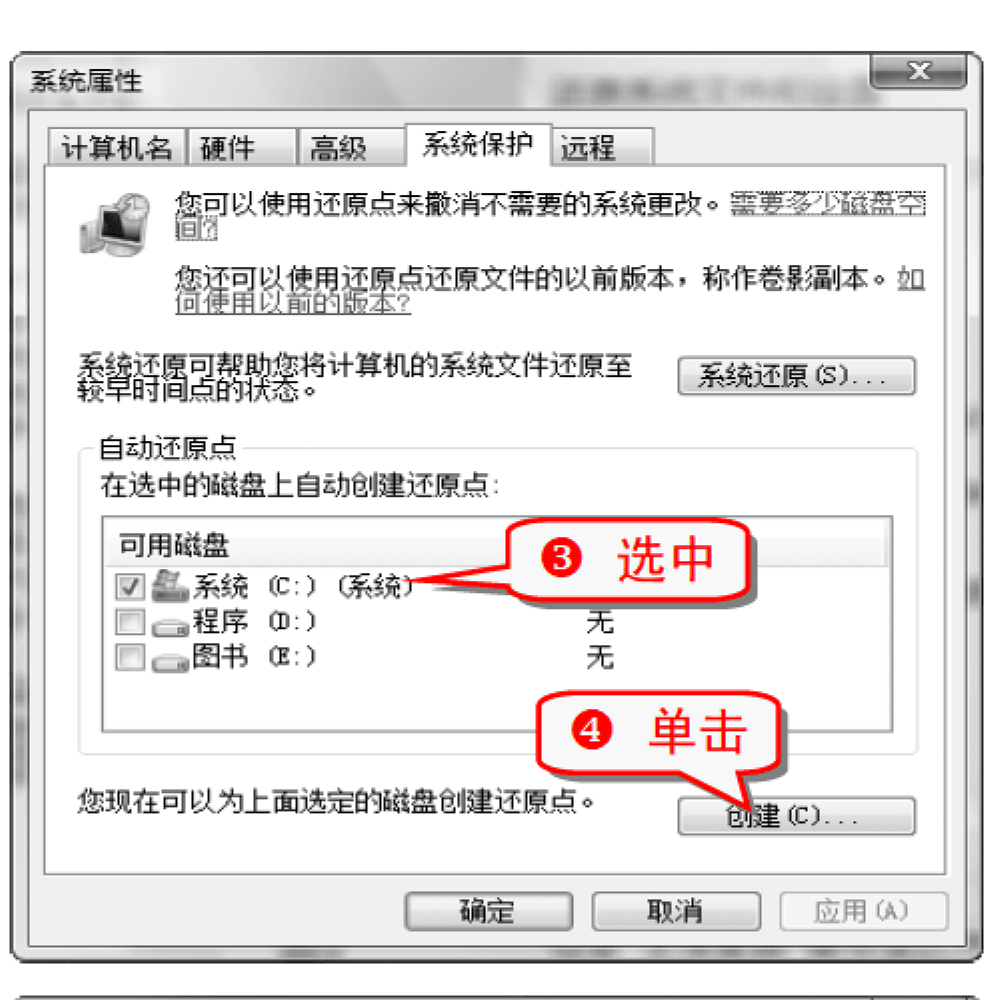
- 创建系统还原点
- 备份系统盘
- 备份和还原注册表
- 备份系统重要文件
- 备份与刷新 BIOS
- 备份驱动程序

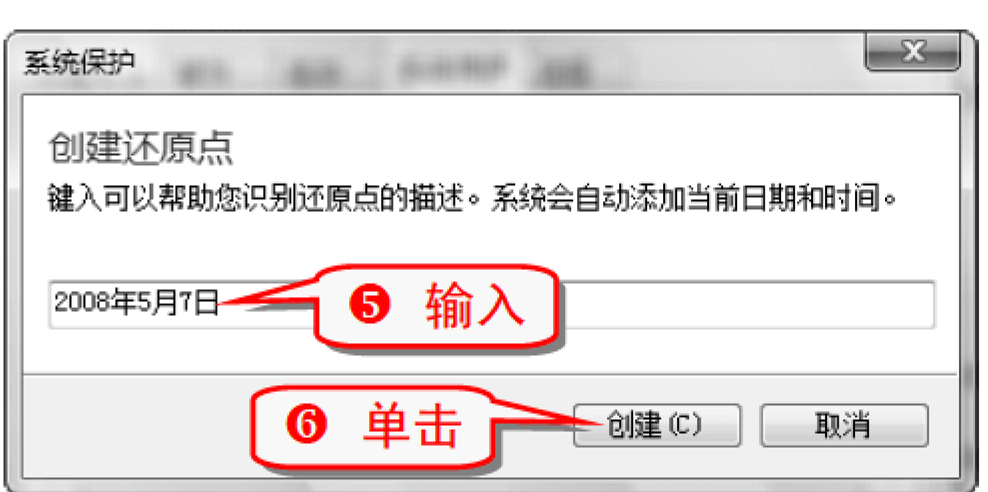
技巧323　手动创建系统还原点

在 Windows Vista 系统中利用系统还原可以将电脑还原到一个较早时间的设置，解决因为误装驱动程序或误删系统文件造成的各种故障。手动创建系统还原点的操作步骤如下。

❶ 右击桌面上的“计算机”图标，在弹出的快捷菜单中选择“属性”命令。



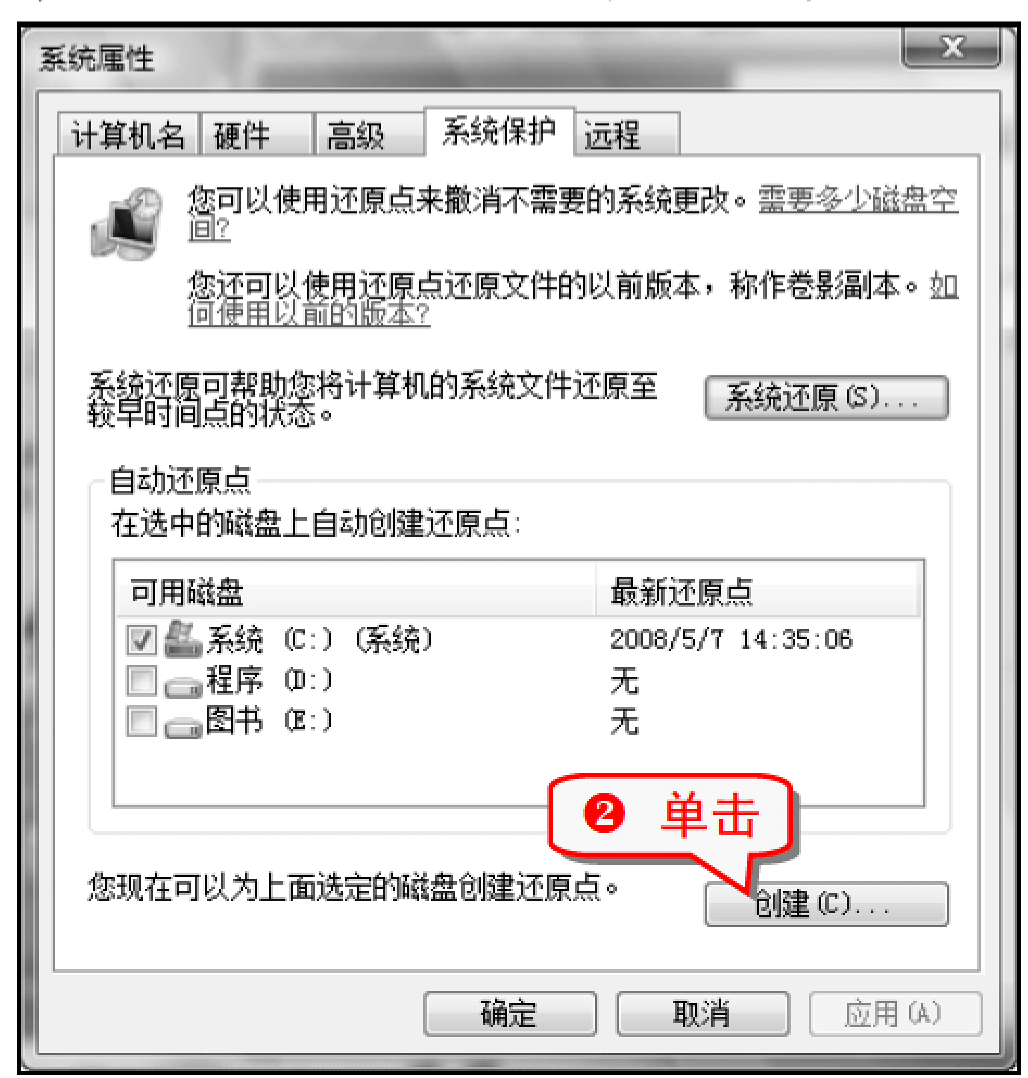


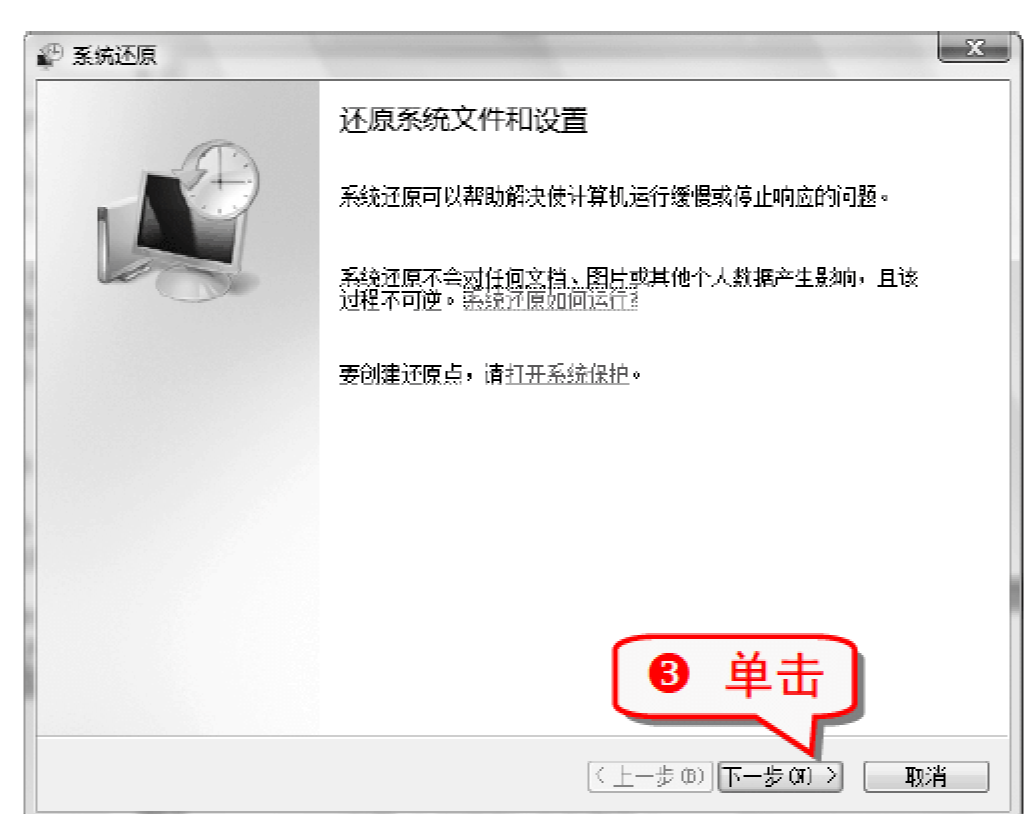


技巧324 使用系统还原点还原系统

在 Windows Vista 系统中当系统发生严重故障的时候，可以通过系统还原点将系统还原到某个原点。

❶ 右击桌面上的“计算机”图标，在弹出的快捷菜单中选择“属性”命令，在弹出的“系统属性”对话框中单击“系统保护”链接，打开“系统属性”对话框。



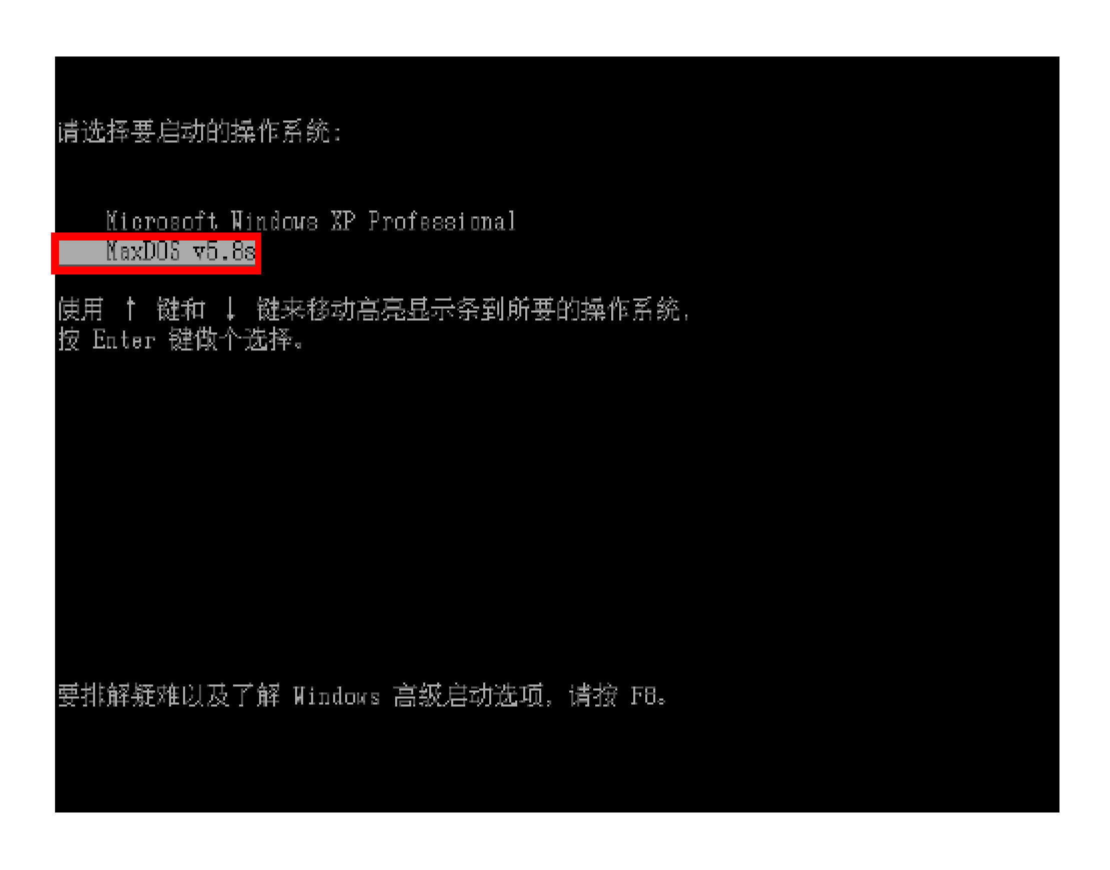




技巧325 使用矮人工具箱备份系统盘

矮人工具箱把矮人 DOS 与 GHOST 工具箱合二为一，成为一个总的集合。使用矮人工具箱进行系统的备份过程简单，一学就会。

❶ 安装好矮人工具箱，重新启动电脑，出现一个 Windows XP 系统和 MaxDOS 的选择界面。



❷ 使用↑和↓键选择 MaxDOS v5.8s 选项，按下 Enter 键，弹出如下界面。



❸ 使用↑和↓键选择“运行 MaxDOS v5.8s”选项，按下 Enter 键，弹出如下界面。

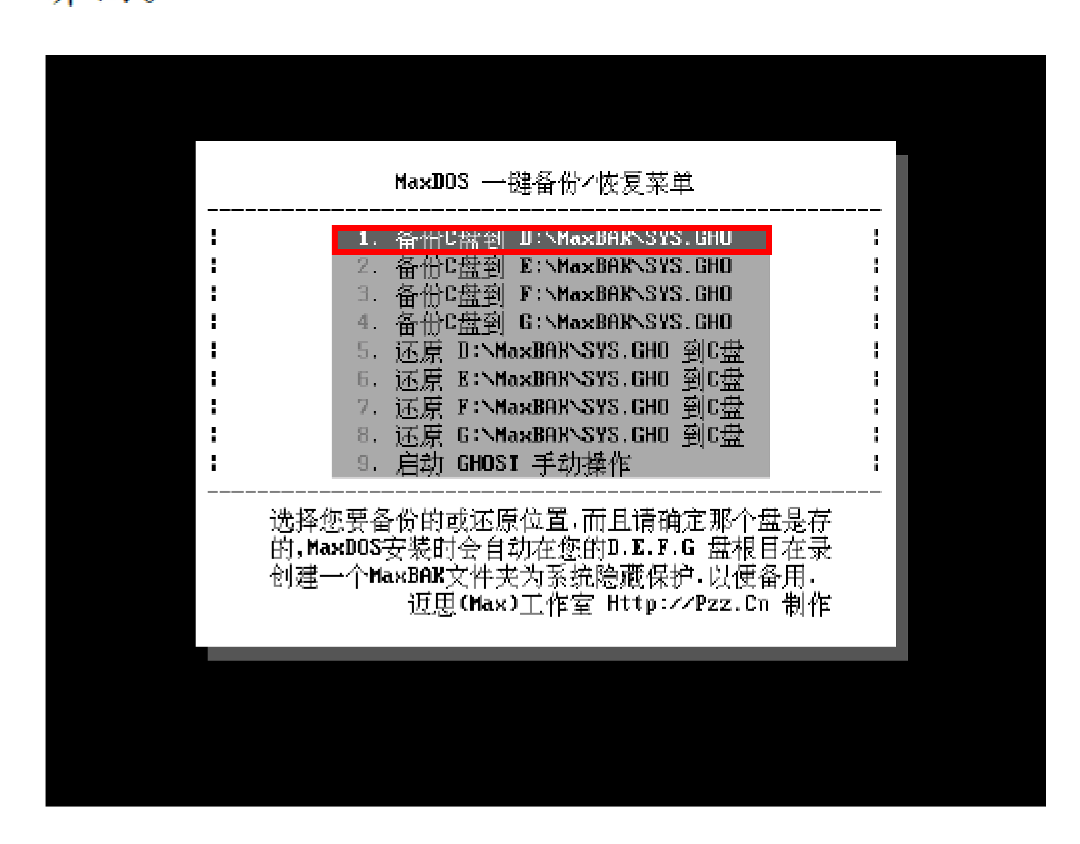


❹ 在 Password: 后面输入密码，并按下 Enter 键(矮人工具箱的默认密码是 max)，弹出如下界面。

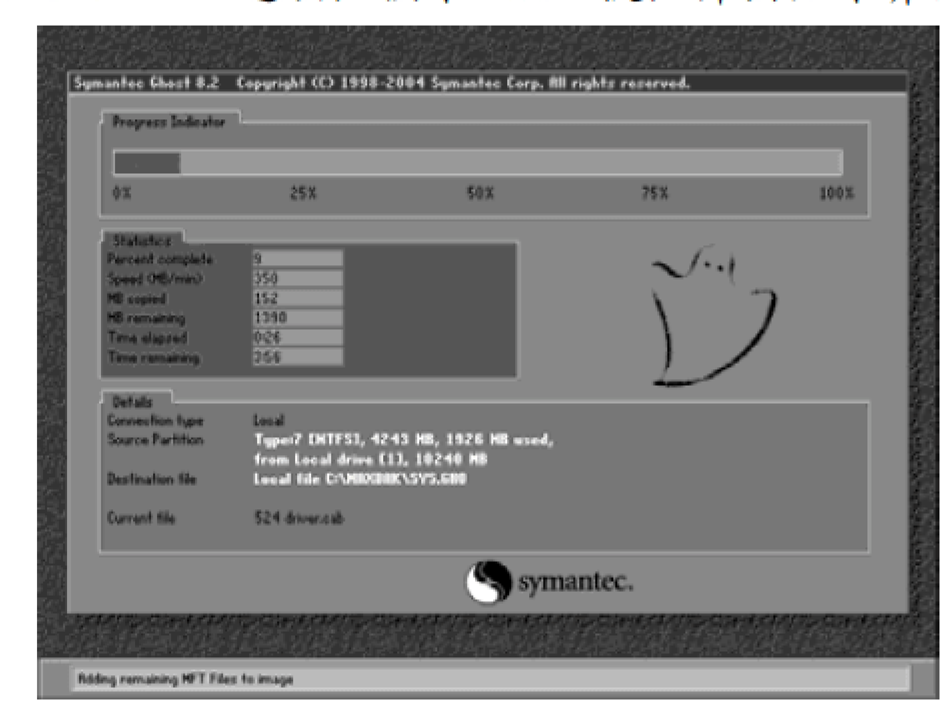




❺ 使用↑和↓键选择“C.备份/还原系统& BACKUP/RESTORE SYSTEM”选项，按下 Enter 键，弹出如下界面。



❻ 使用↑和↓键选择“1.备份 C 盘到 D:\MaxBAK\SYS.GHO”选项，按下 Enter 键，弹出如下界面。



❼ 等待完成备份以后，系统会自动重新启动。

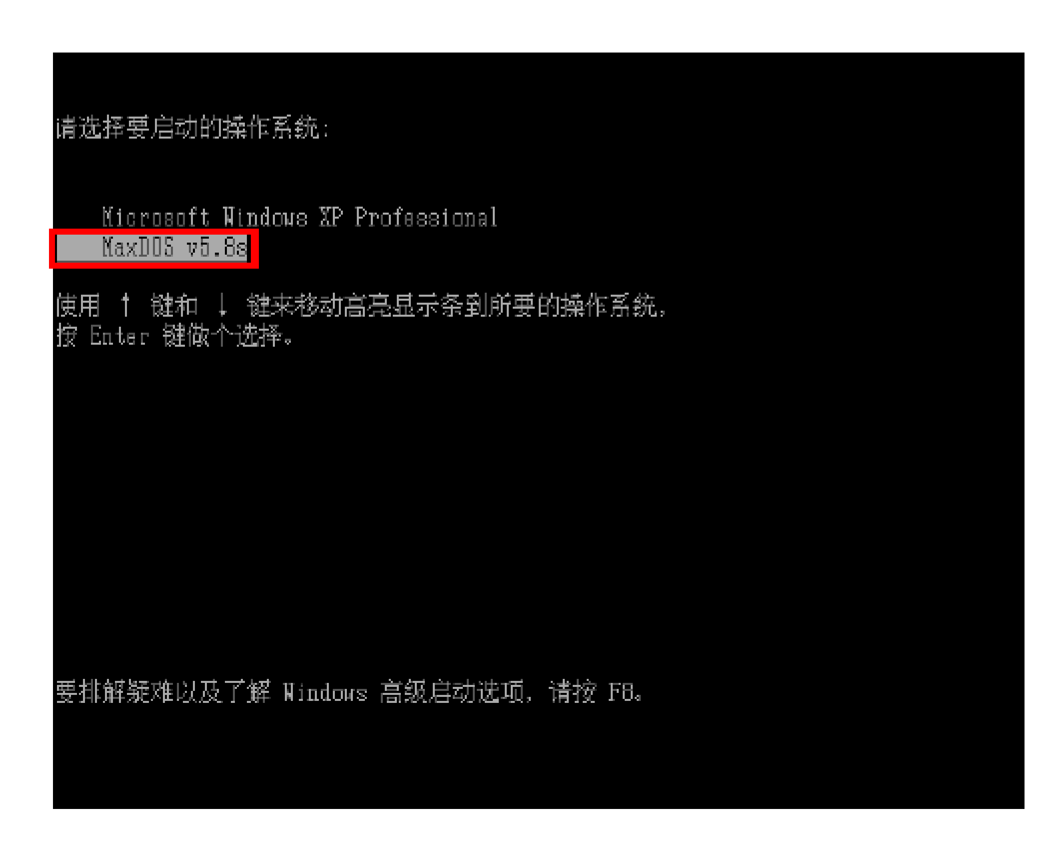


备份的文件不能存放在系统盘中，此外，矮人工具箱不适合 Windows Vista 的系统备份。

技巧326　使用矮人工具箱还原系统

还原系统的步骤跟备份系统的步骤相似。

❶ 重新启动电脑，在选择界面中使用↑和↓键选择 MaxDOS v5.8s 选项，按下 Enter 键。



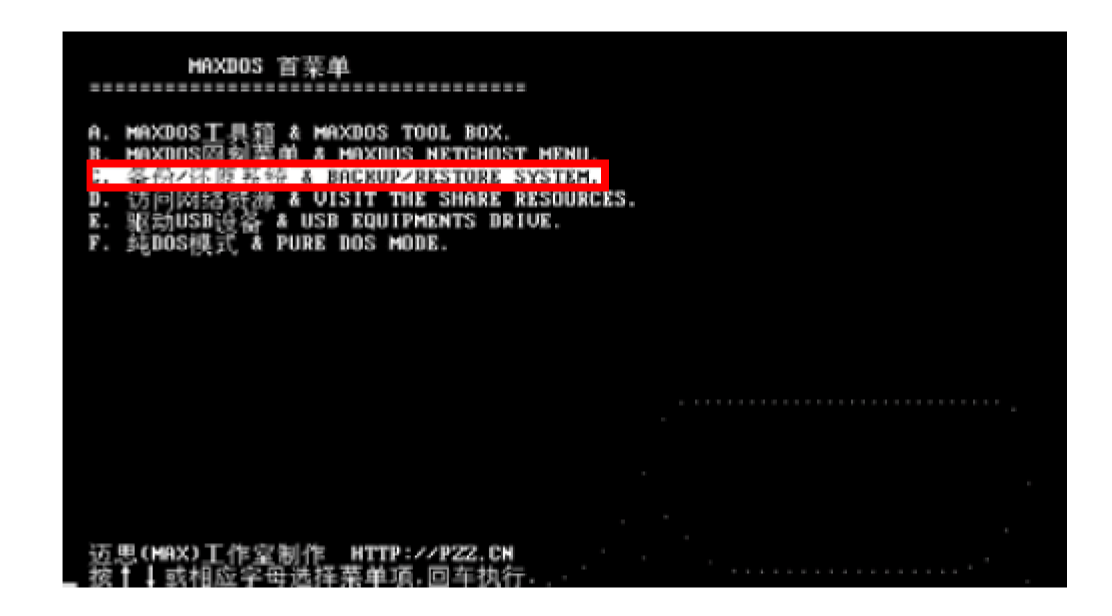
❷ 使用↑和↓键选择“运行 MaxDOS v5.8s”选项，按下 Enter 键。



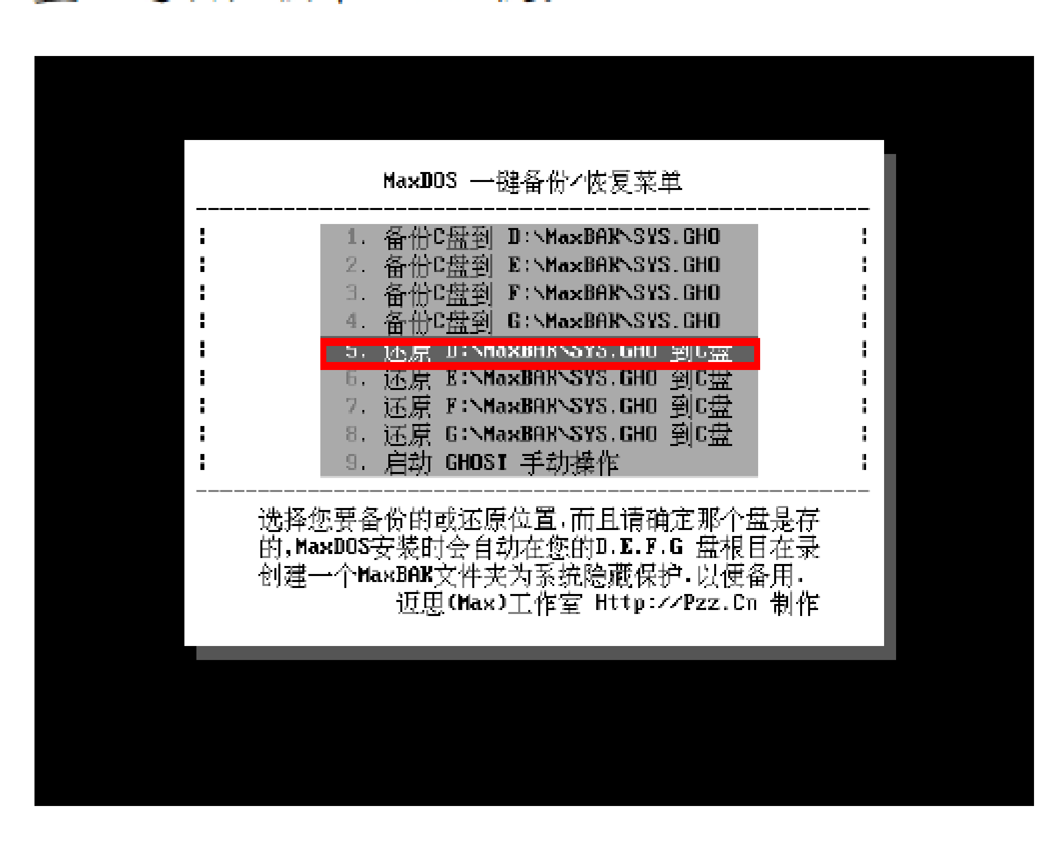
❸ 在 Password: 后面输入密码，并按下 Enter 键。



❹ 使用↑和↓键选择“C. 备份/还原系统& BACKUP/RESTORE SYSTEM”选项，按下 Enter 键。

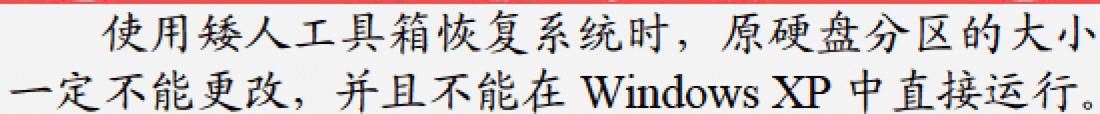


❺ 使用↑和↓键选择“5.还原 D:\MaxBAK\SYS.GHO 到 C 盘”选项，按下 Enter 键。



❻ 等待完成还原以后，系统会自动重新启动。





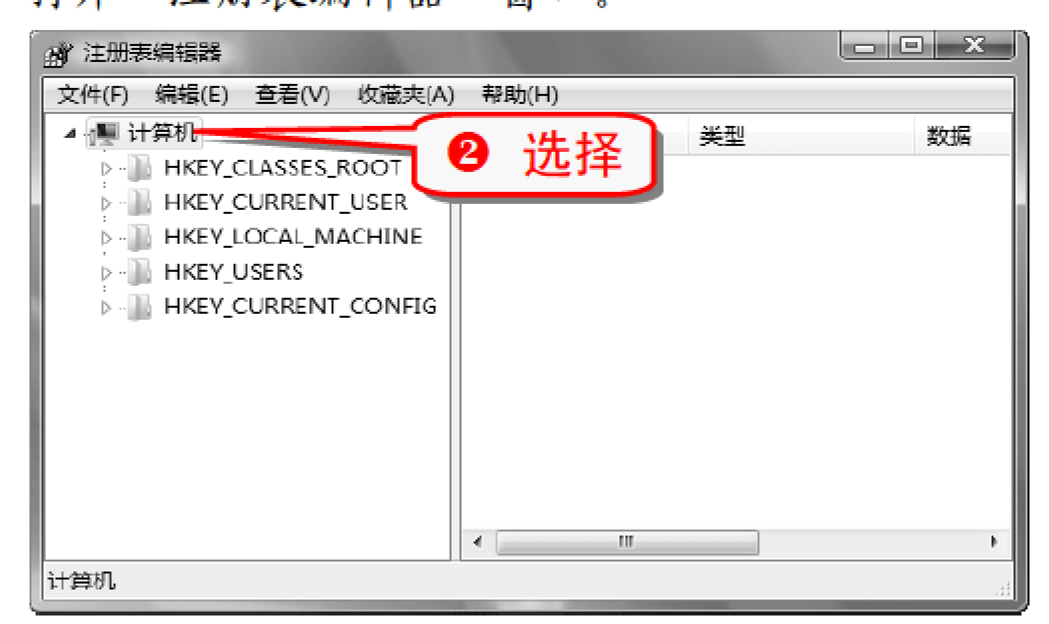
使用矮人工具箱恢复系统时，原硬盘分区的大小一定不能更改，并且不能在 Windows XP 中直接运行。

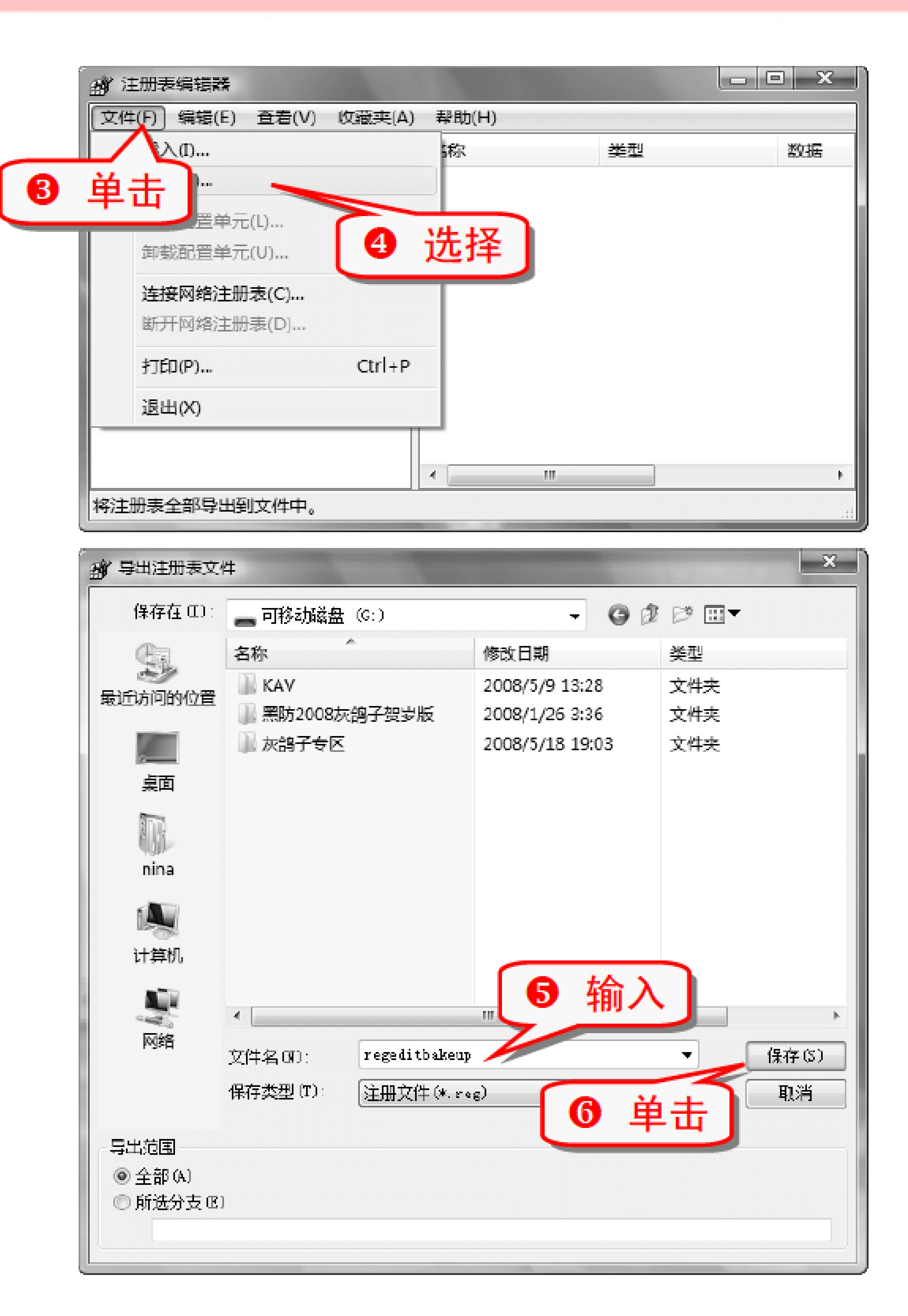
技巧327　备份和恢复注册表

注册表如果遭到破坏，Windows 系统将不能正常的工作，为了确保 Windows 系统的安全，需要对注册表进行备份，备份和恢复注册的操作如下。

(1) 备份注册表

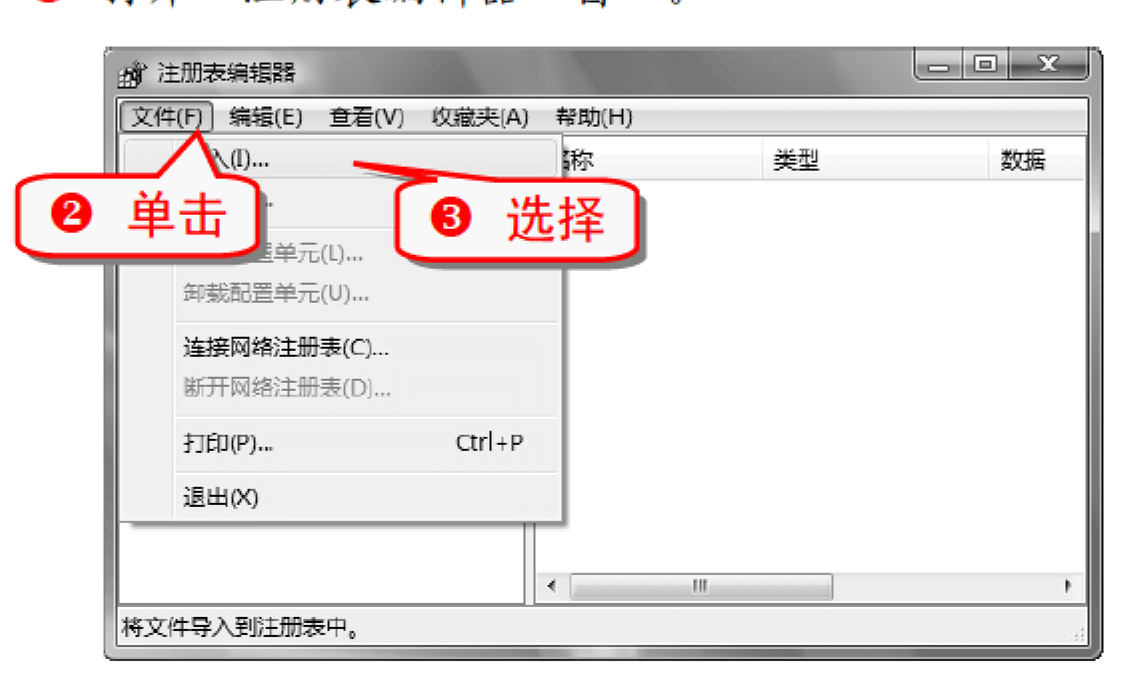
❶ 打开“注册表编辑器”窗口。

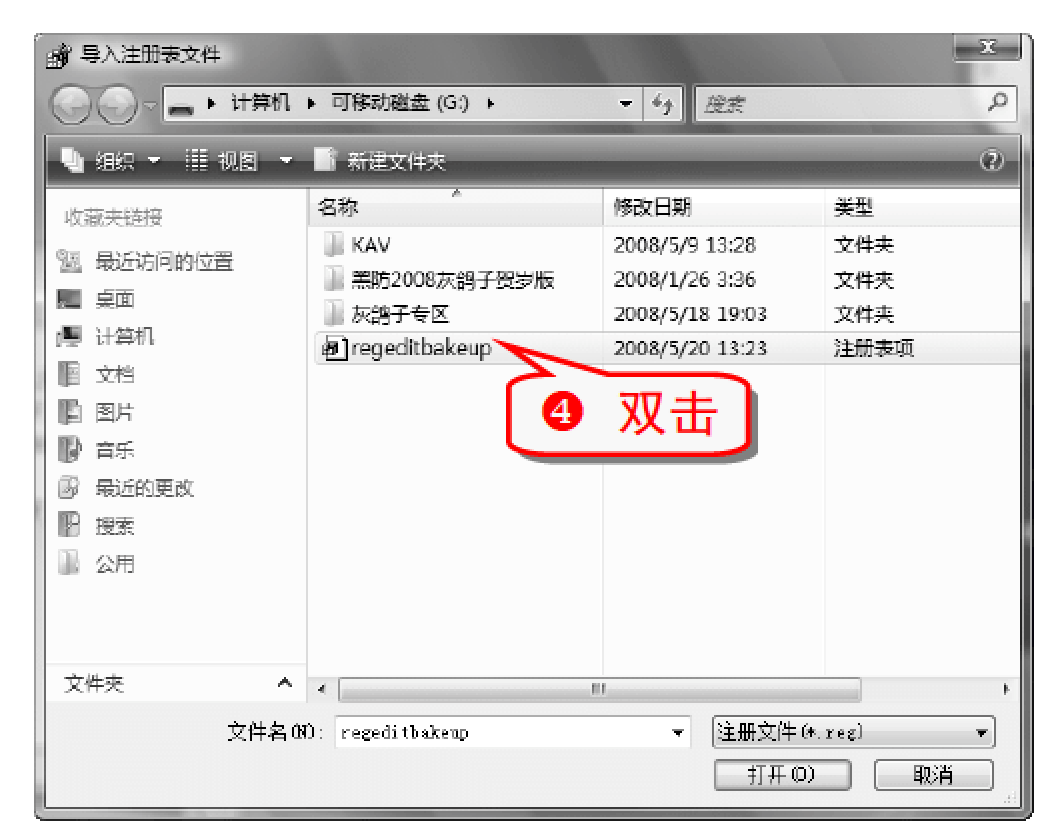




(2) 恢复注册表

❶ 打开“注册表编辑器”窗口。





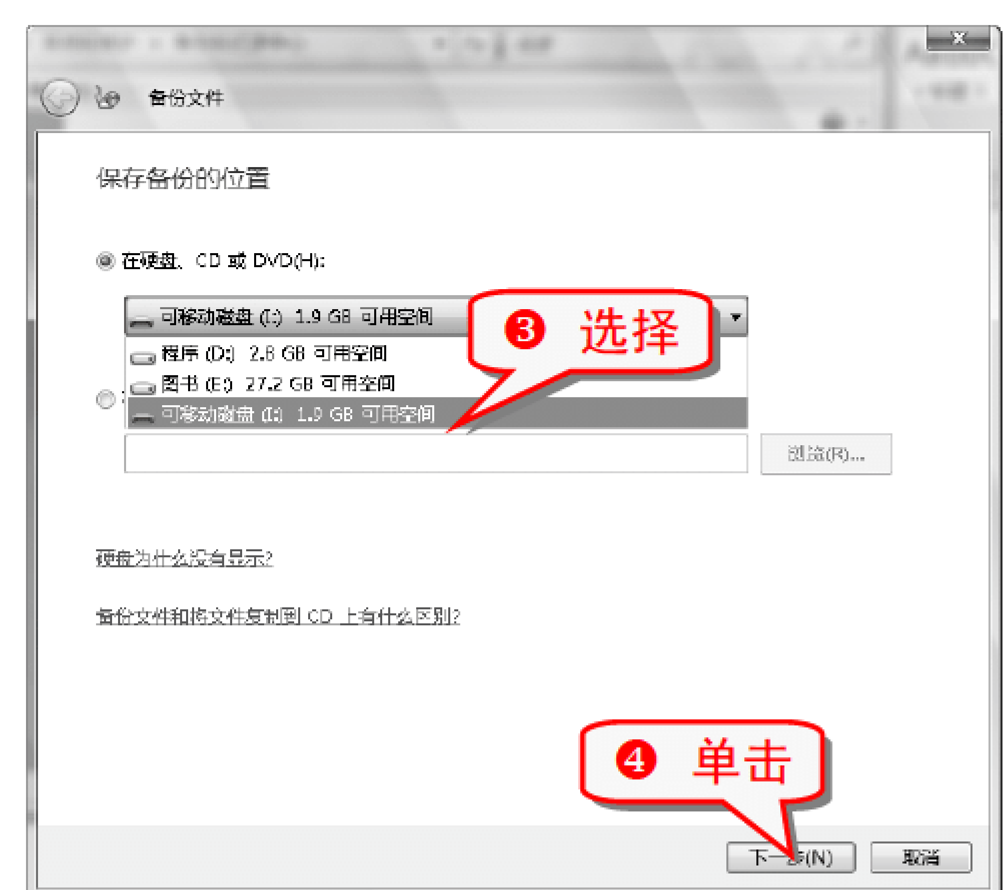


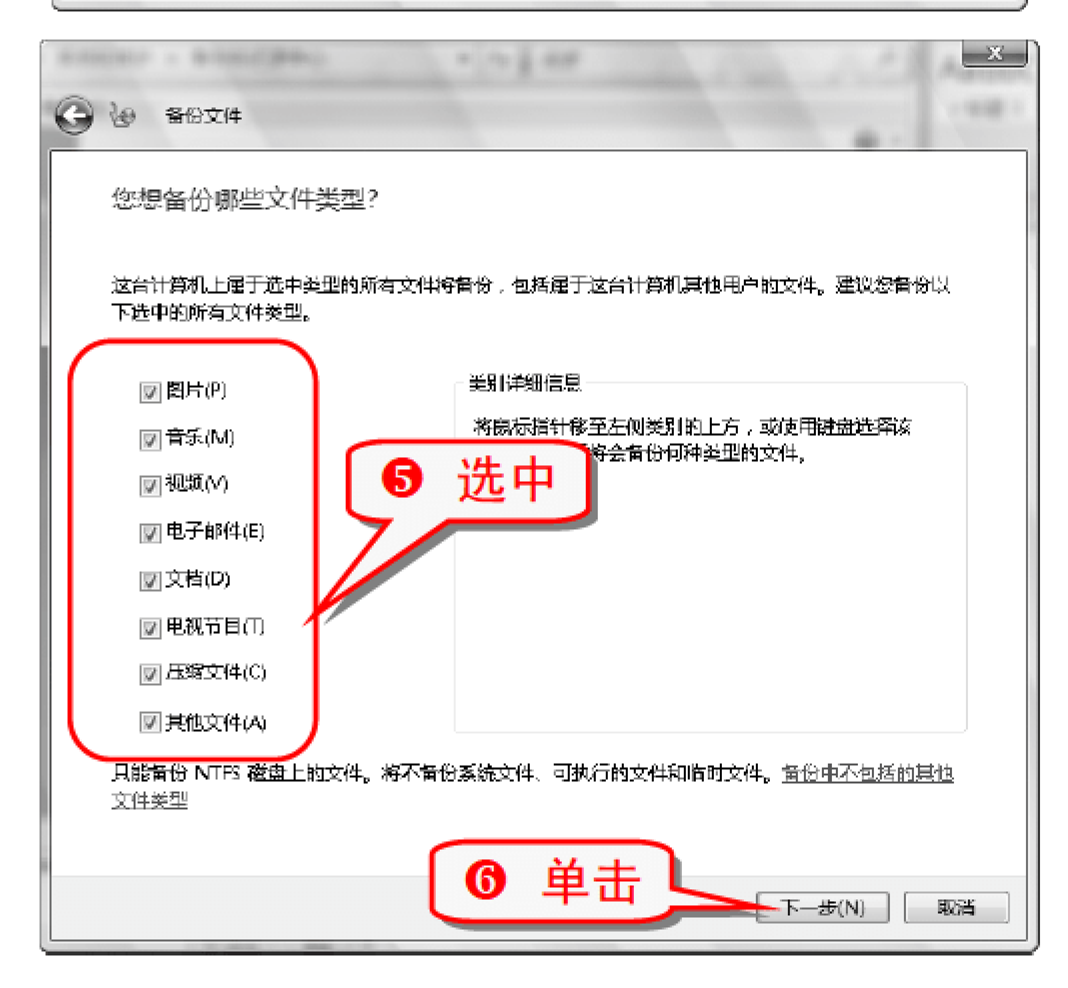
技巧328　备份系统重要文件

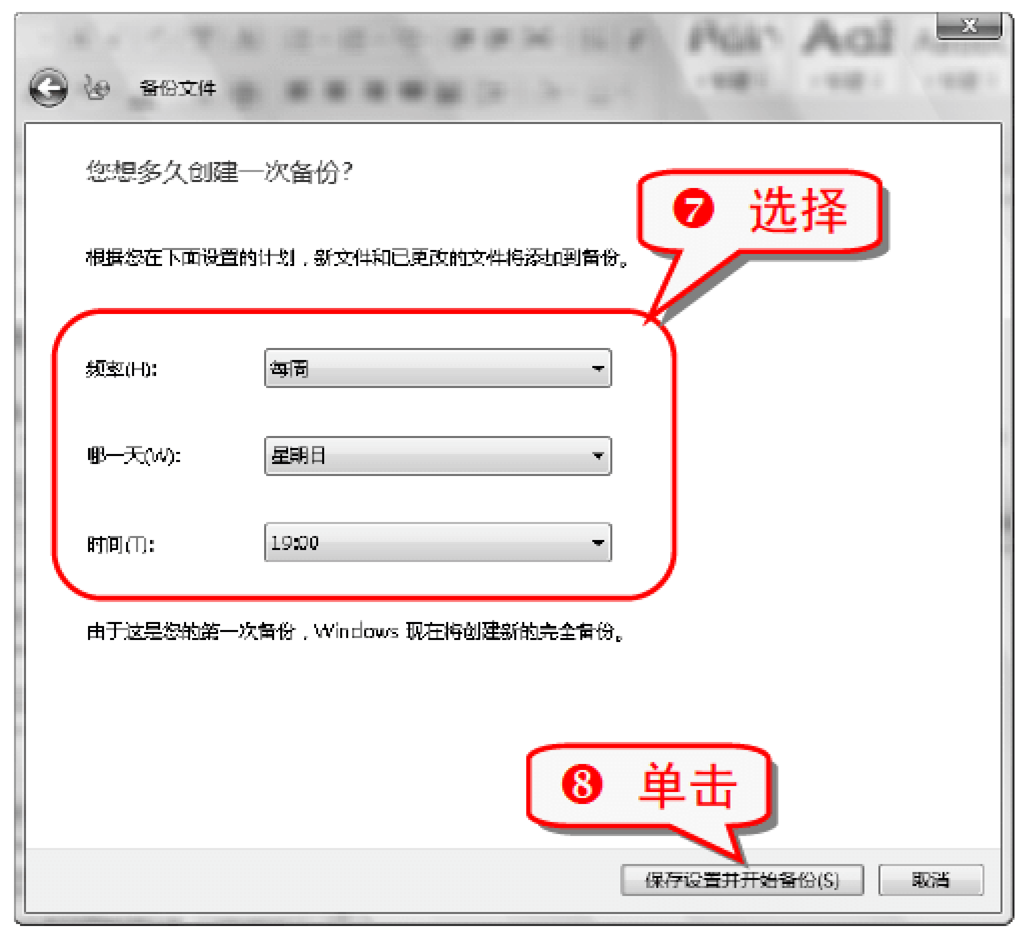
由于多个用户共同使用一台电脑或操作不慎可能导致系统出错，这样就很有必要对系统的重要文件进行备份，当系统出现问题时，可以使用备份盘来恢复系统的重要数据。

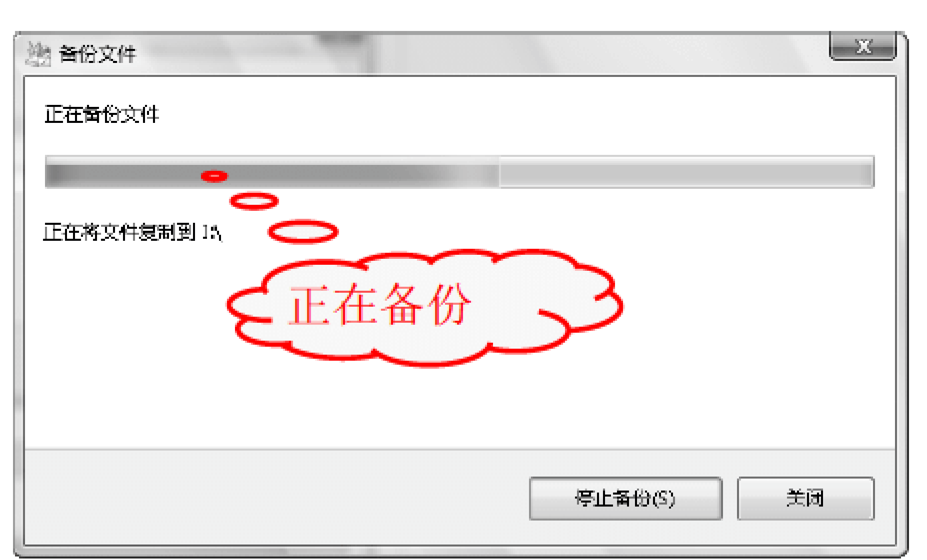
❶ 在打开的控制面板中单击“系统和维护”→“备份和还原中心”链接，弹出“备份和还原中心”窗口。













注　意　事　项

在选择“保存备份的位置”时，最好是保存在外部磁盘，这样即使整个系统崩溃了重要的数据也不会丢失，可以将文件导入到其他的电脑中进行还原。

技巧329　还原系统重要文件

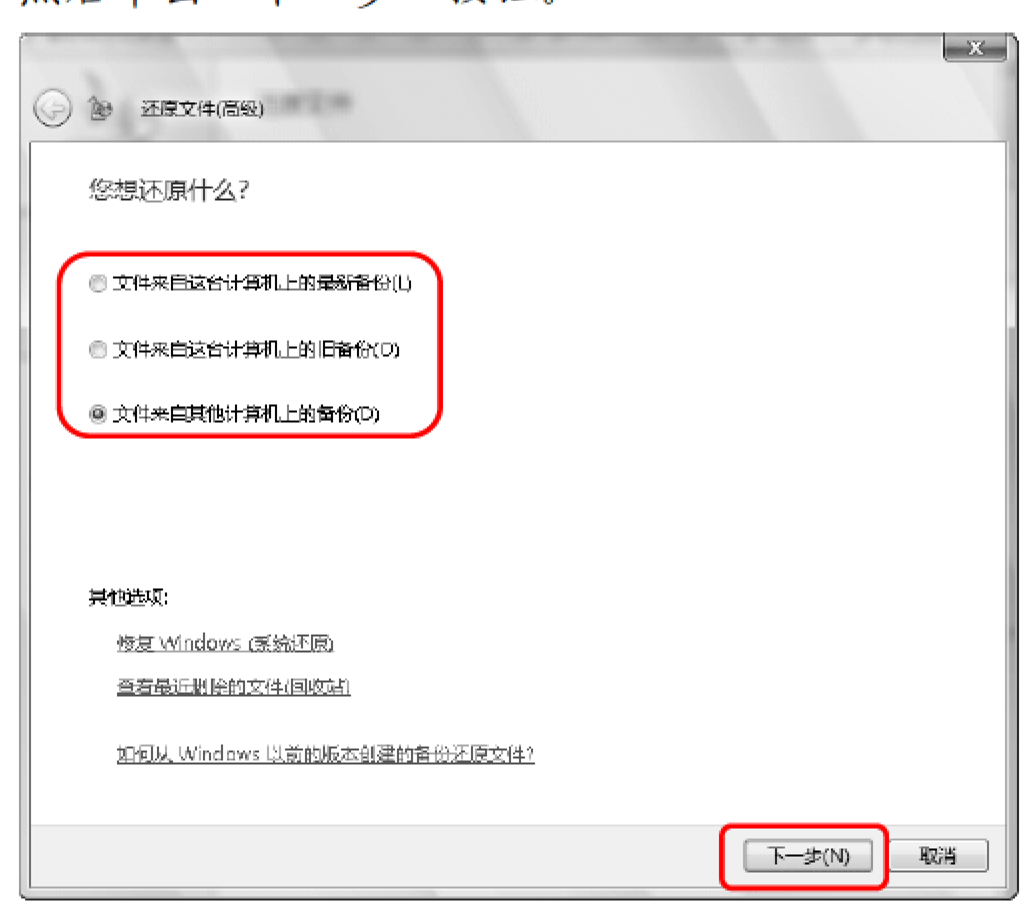
Windows Vista 系统有时也会出现数据被破坏的情况，用户可以通过紧急救助盘对整个系统或被破坏的数据进行还原。

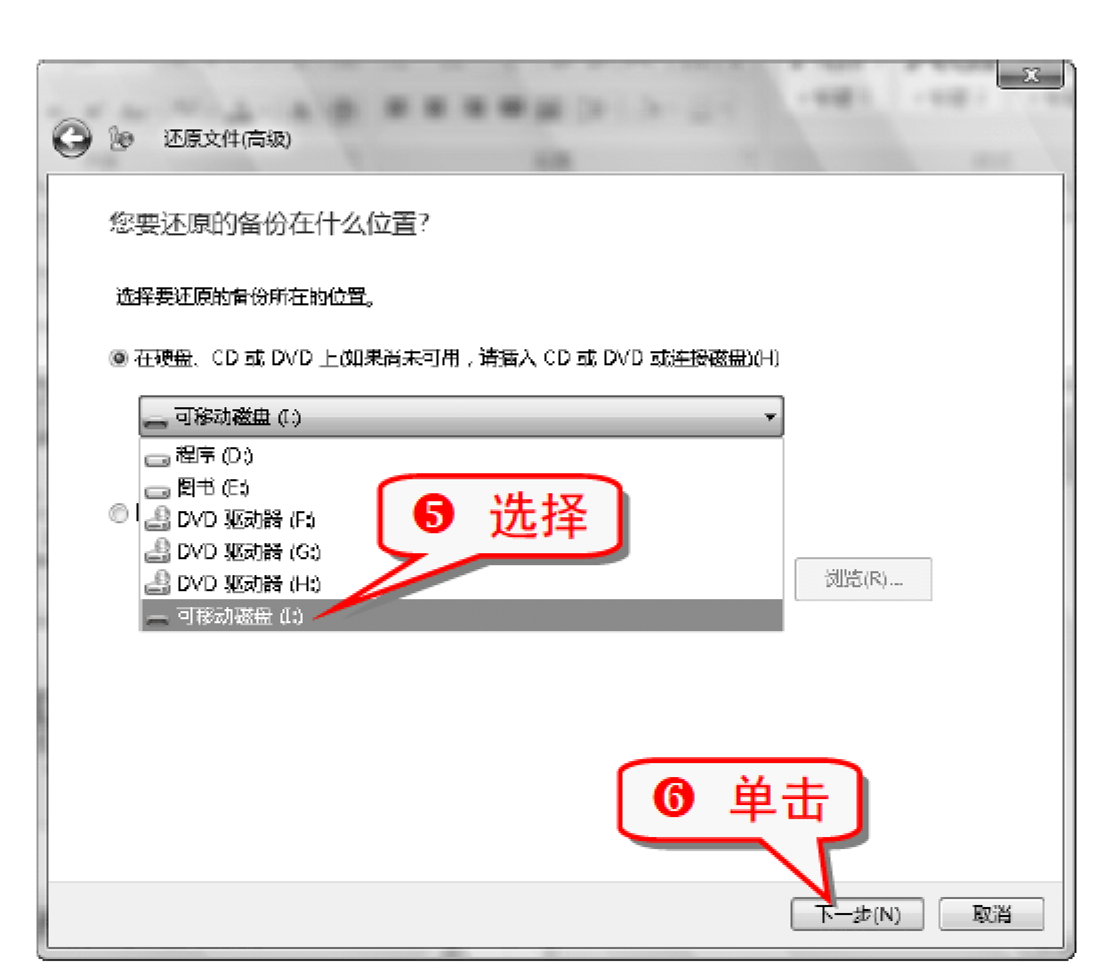
❶ 在打开的控制面板中单击“系统和维护”→“备份和还原中心”链接，弹出“备份和还原中心”窗口。



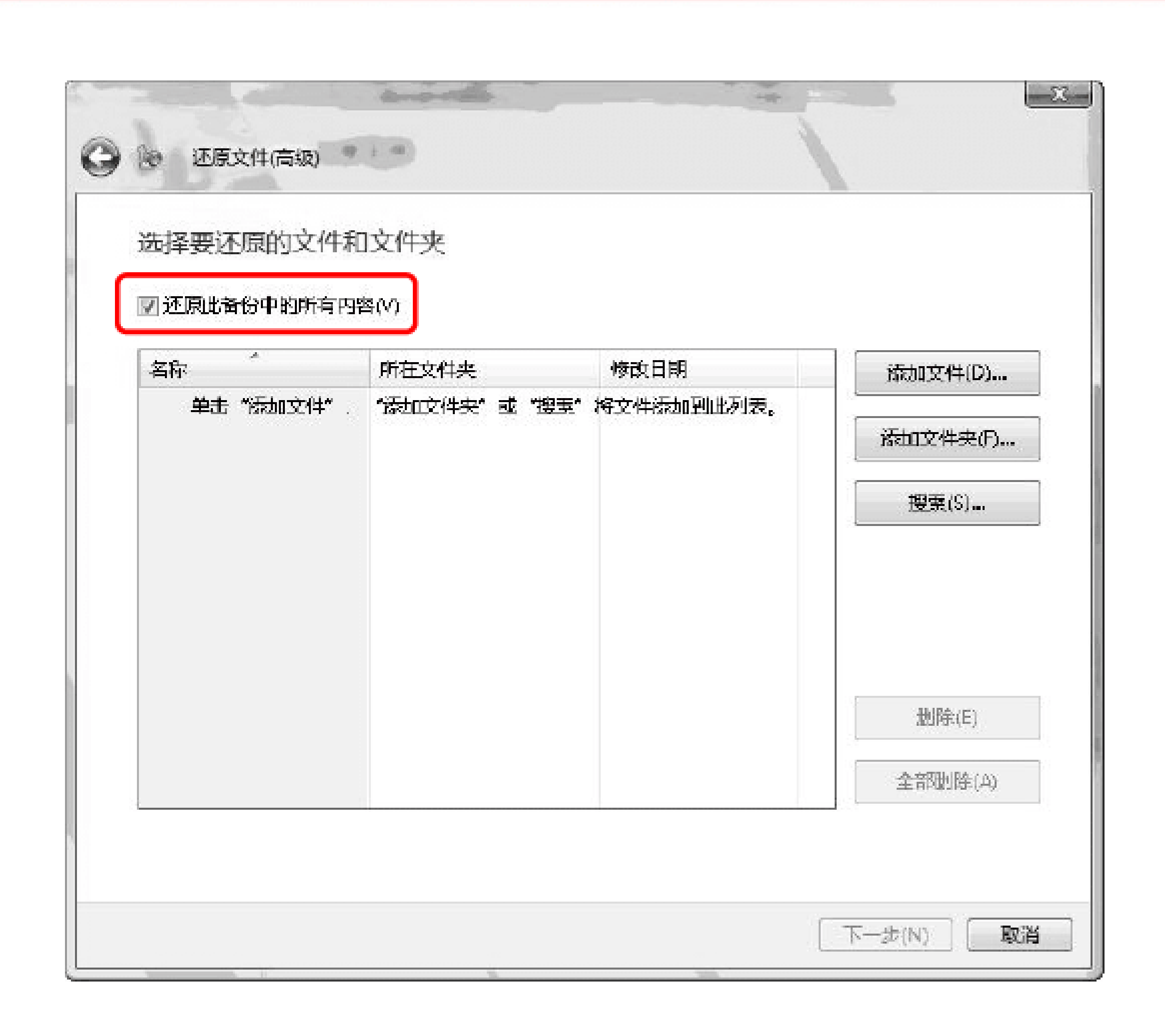


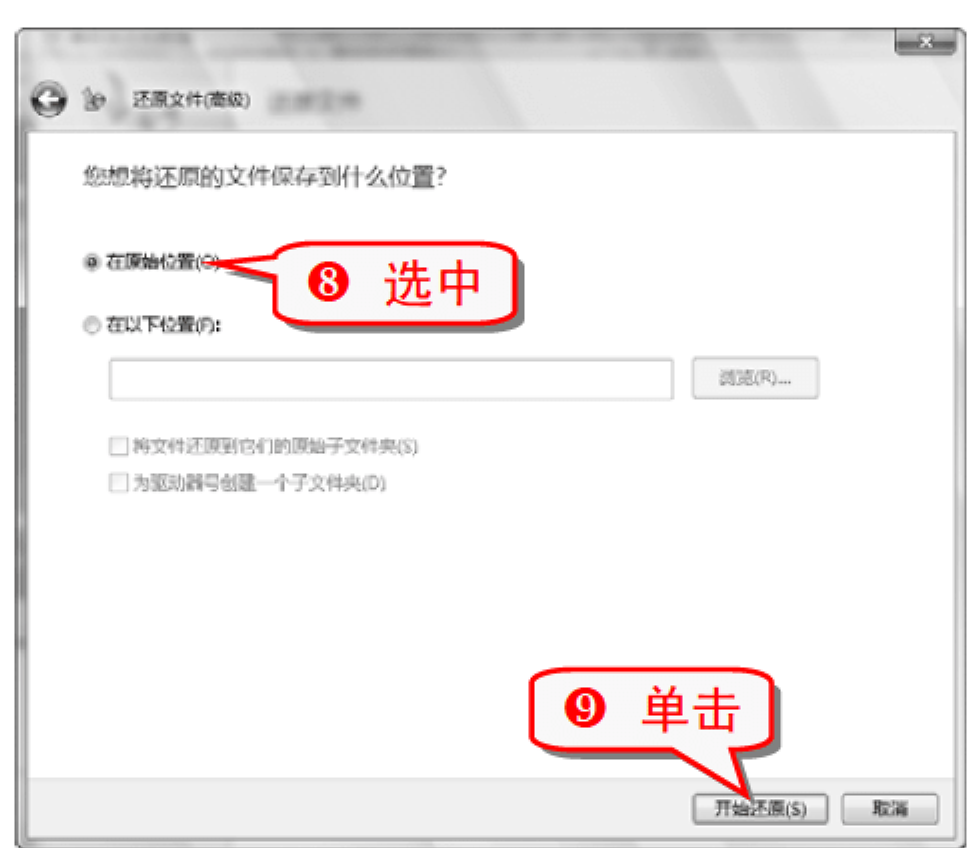
❹ 在“您想还原什么”界面中，选择备份数据的来源，然后单击“下一步”按钮。

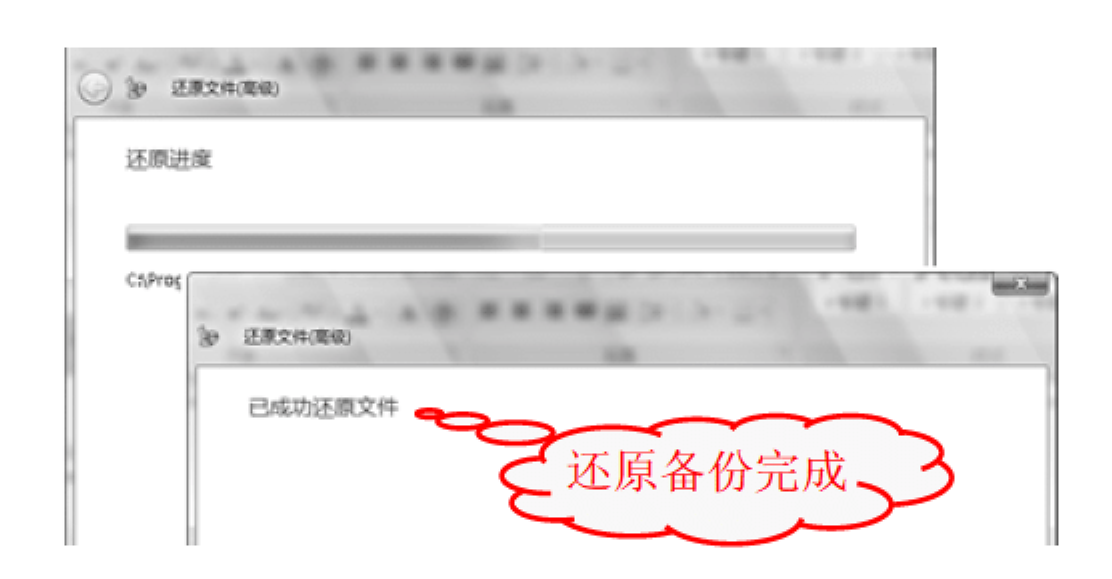




❼ 在“选择要还原的文件和文件夹”界面中，选中“还原此备份中的所有内容”复选框，弹出“您想将还原的文件保存到什么位置”界面。







注 意 事 项

第❼步操作时，在“选择要还原的文件和文件夹”界面中，选中“还原此备份中的所有内容”复选框，因为不能确定具体哪些数据已经被破坏，还原的时候只要将原来的文件覆盖即可。

技巧330 创建 Windows Complete PC 备份

创建 Windows Complete PC 备份将会创建整个计算机副本，包括程序、系统程序和文件。



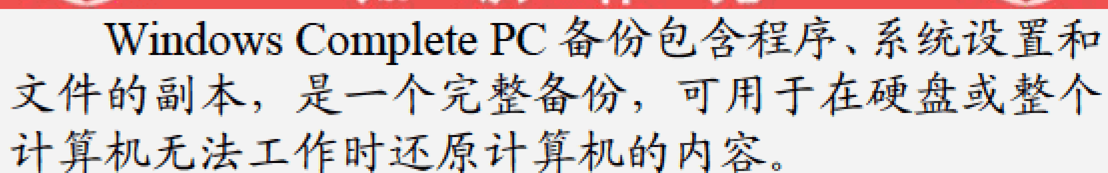
❶ 打开「开始」菜单，选择“所有程序”→“附件”→“系统工具”→“备份状态和设置”命令。











Windows Complete PC 备份包含程序、系统设置和文件的副本，是一个完整备份，可用于在硬盘或整个计算机无法工作时还原计算机的内容。

从 Windows Complete PC 备份映象中还原计算机时，将进行完整还原，不能选择个别项进行还原。

技巧331　备份与刷新 BIOS

备份 BIOS 等系统信息在重装系统或者系统崩溃时可以进行快速还原，减小数据损失。

刷新 BIOS，即升级主板 BIOS，可以修正以前版本中的漏洞，获得对新的硬件设备或技术规范的支持；解决一些特殊的计算机故障；提高计算机的性能。在刷新 BIOS 前需要对 BIOS 进行备份，这样在 BIOS 刷新失败时，可以正常恢复启动。

技嘉科技的@BIOS 软件，可以实现主板 BIOS 的在线升级。这是首款 Windows 在线更新的 BIOS 工具，是一个智能化的 BIOS 更新软件，可以帮助用户从 Internet 上下载对应的 BIOS 程序，并将其更新，是一个 Windows 自动下载的工具。

更新 BIOS 时，只需单击鼠标，便可以更新到最新版本的 BIOS。该工具可以检测到用户主板的型号，帮助用户选择适合的 BIOS 文件，并自动到最新的技嘉 FTP 站点上去下载。

(1) @BIOS 工具软件下载

在 http://www.gigabyte.com.cn/ 网站上下载@BIOS 软件，文件名为 biosflashl06g.exe。下载完毕后，双击执行，程序即可自动监测主板信息，并显示在启动窗口中。

注　意　事　项



该软件只适用于支持在线更新功能的技嘉主板，需要仔细察看主板说明书看电脑是否支持该软件。

(2) 备份 BIOS 文件

在起始的对话框中，单击 Save Current BIOS 按钮，在弹出的对话框中保存目前版本的 BIOS 信息。

(3) 通过 Internet 更新 BIOS

❶ 选中 Internet Update 复选框。

❷ 单击 Update New BIOS 按钮。

❸ 选择“@BIOS 服务器”选项。

❹ 选择使用的主板的正确型号。

❺ 系统自动下载 BIOS 文件，然后按照提示完成更新操作。

(4) 在 Windows 下直接更新 BIOS

❶ 取消 Internet Update 复选框。

❷ 单击 Update New BIOS 按钮。

❸ 在“打开文件”对话框中，将文件类型设置为 All Files(*.*)。

❹ 找到通过网站下载的或其他渠道得到的并已解压缩的 BIOS 文件，然后按照提示完成更新操作。



注 意 事 项

使用@BIOS 注意事项：

- 在上述操作中，如果出现两个或两个以上的型号供选择，需再次确认。因为选错主板型号更新 BIOS，会导致系统无法开机。
- Windows 直接更新时，已解压缩的 BIOS 文档所属的主板型号，要与自己的主板型号相符，否则会导致系统无法开机。
- 在线更新时，如果@BIOS 服务器找不到自己主板型号的 BIOS 文档，则到该公司网站下载该主板型号最新版本的 BIOS 文件，解压缩后，利用 Windows 直接更新的方法来更新 BIOS。
- 在更新 BIOS 的过程中，不能中断，否则会导致系统无法开机。

技巧332 Windows Vista 的自动文件备份功能

利用 Windows Vista 系统中的自动文件备份功能可将电脑中最常见的文件类型备份到指定的位置。并且 Windows 会按指定的计划扫描系统，将新的或者更新的文件自动添加到备份之中。

设置自动文件备份可以保护文件，避免意外丢失或者删除文件。



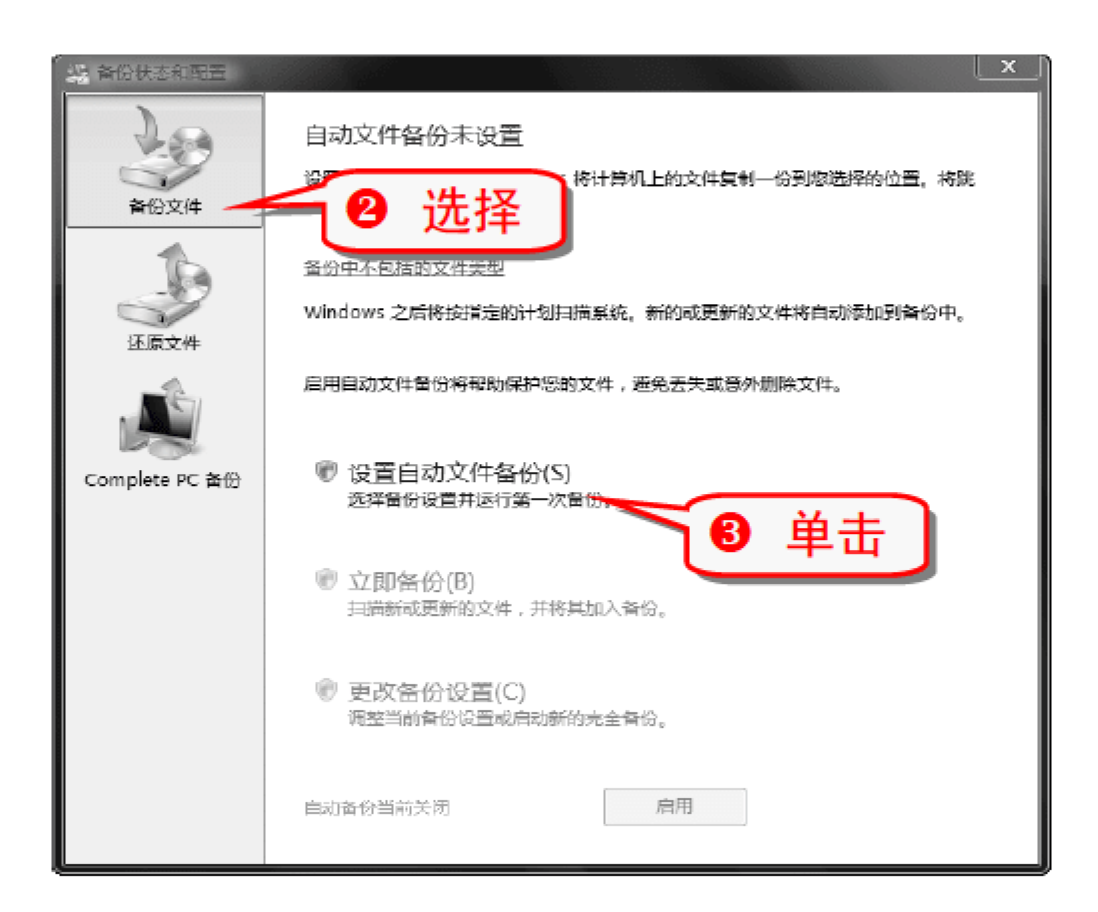

知 识 补 充

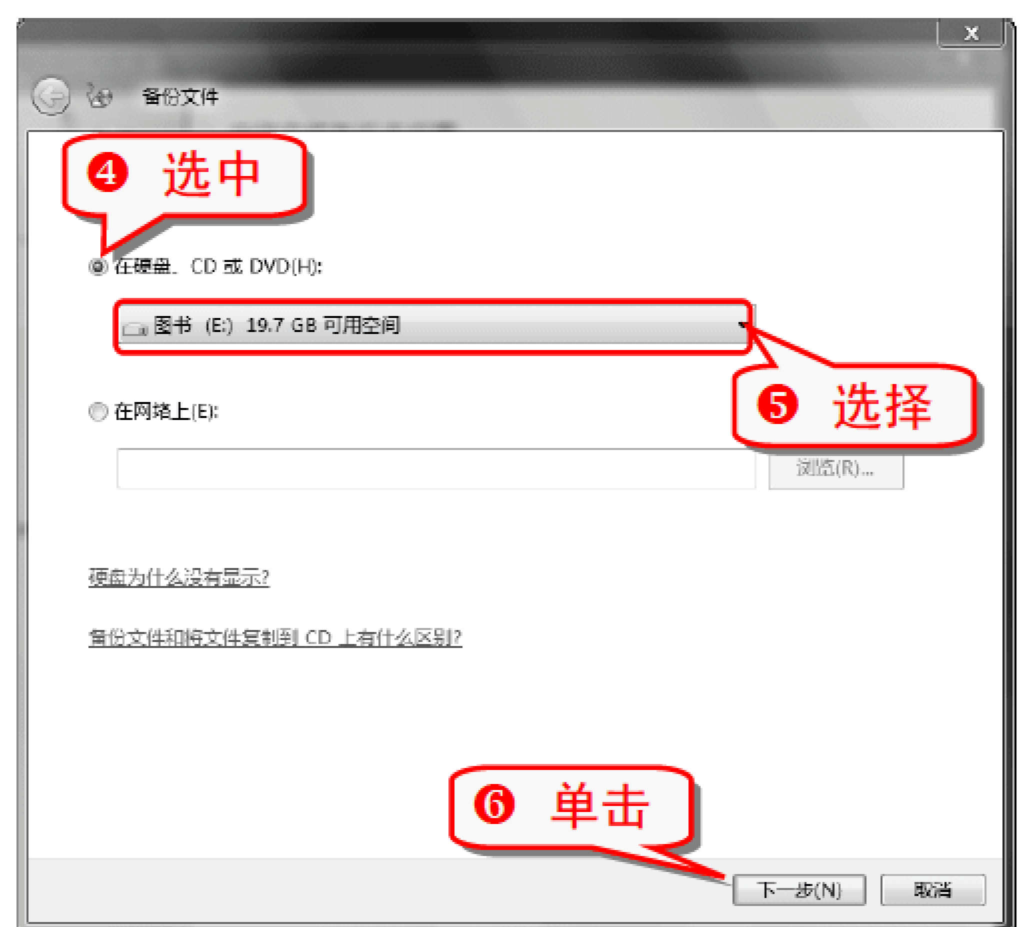
备份文件不包括以下几类文件：

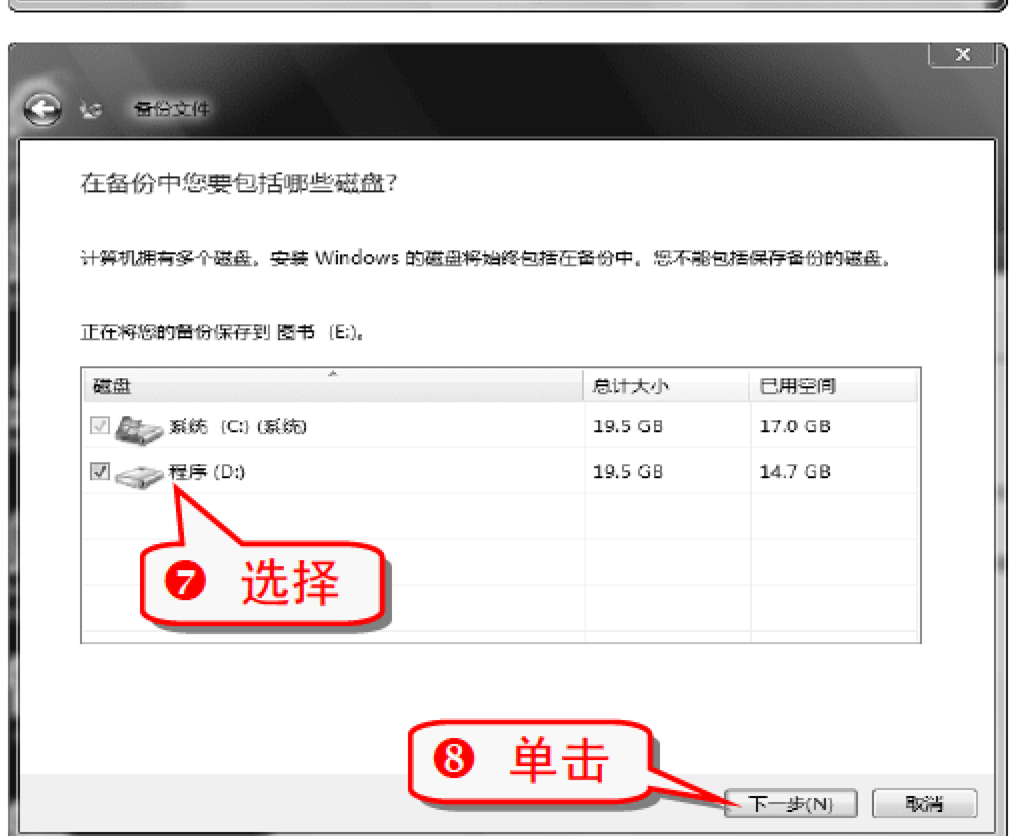
- 已使用加密文件系统(EFS)加密的文件(EFS 未包含在 Windows Vista Starter、Windows Vista Home Basic 和 Windows Vista Home Premium 中)。
- 系统文件(Windows 需要运行的文件)。
- 程序文件。
- 存储在使用 FAT 文件系统格式化的硬盘上的文件。
- 未存储在硬盘上的基于 Web 的电子邮件。
- 回收站中的文件。
- 临时文件。
- 用户配置文件。

(1) 选择备份文件与其存放位置

❶ 打开「开始」菜单，选择“所有程序”→“附件”→“系统工具”→“备份状态和设置”命令。





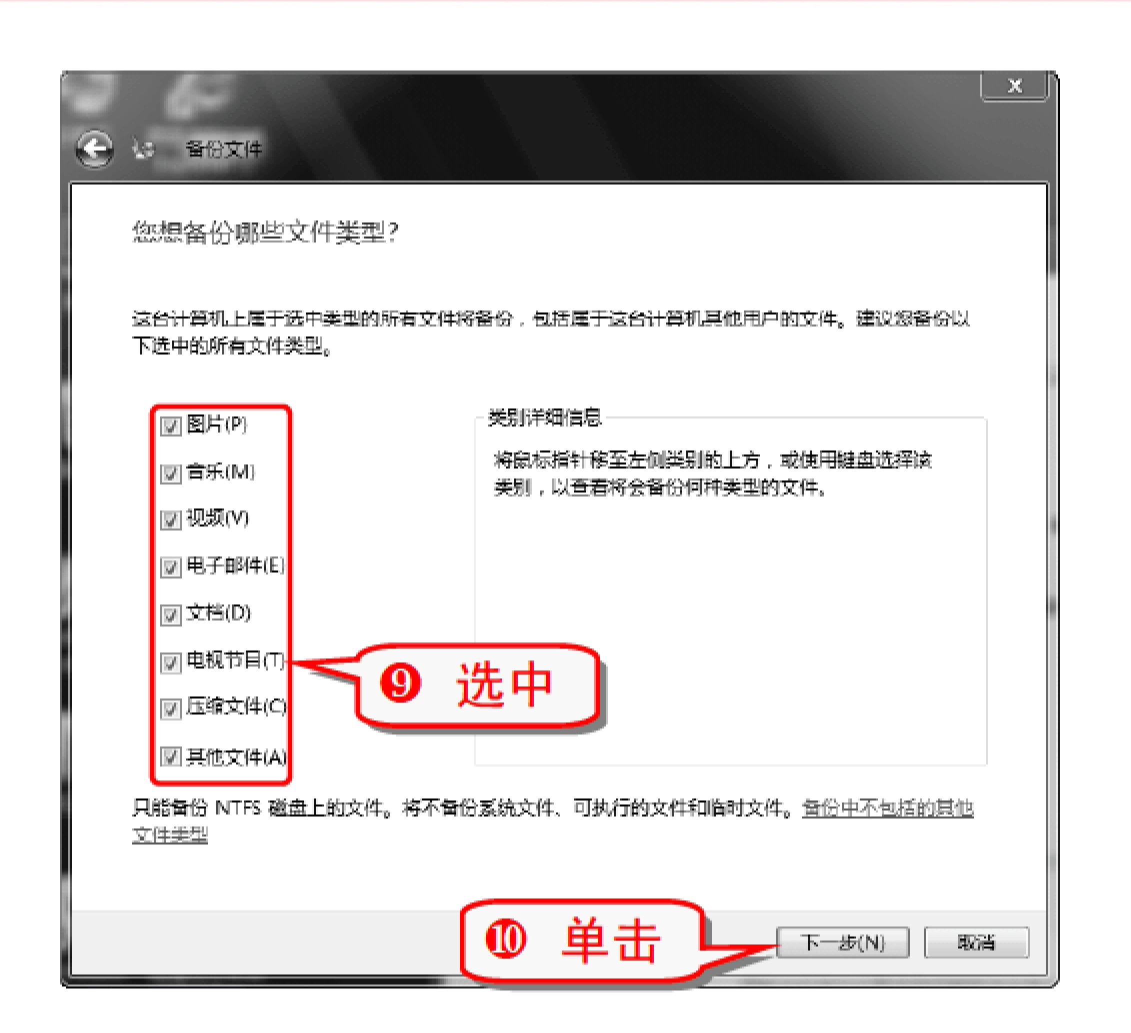




专 家 坐 堂

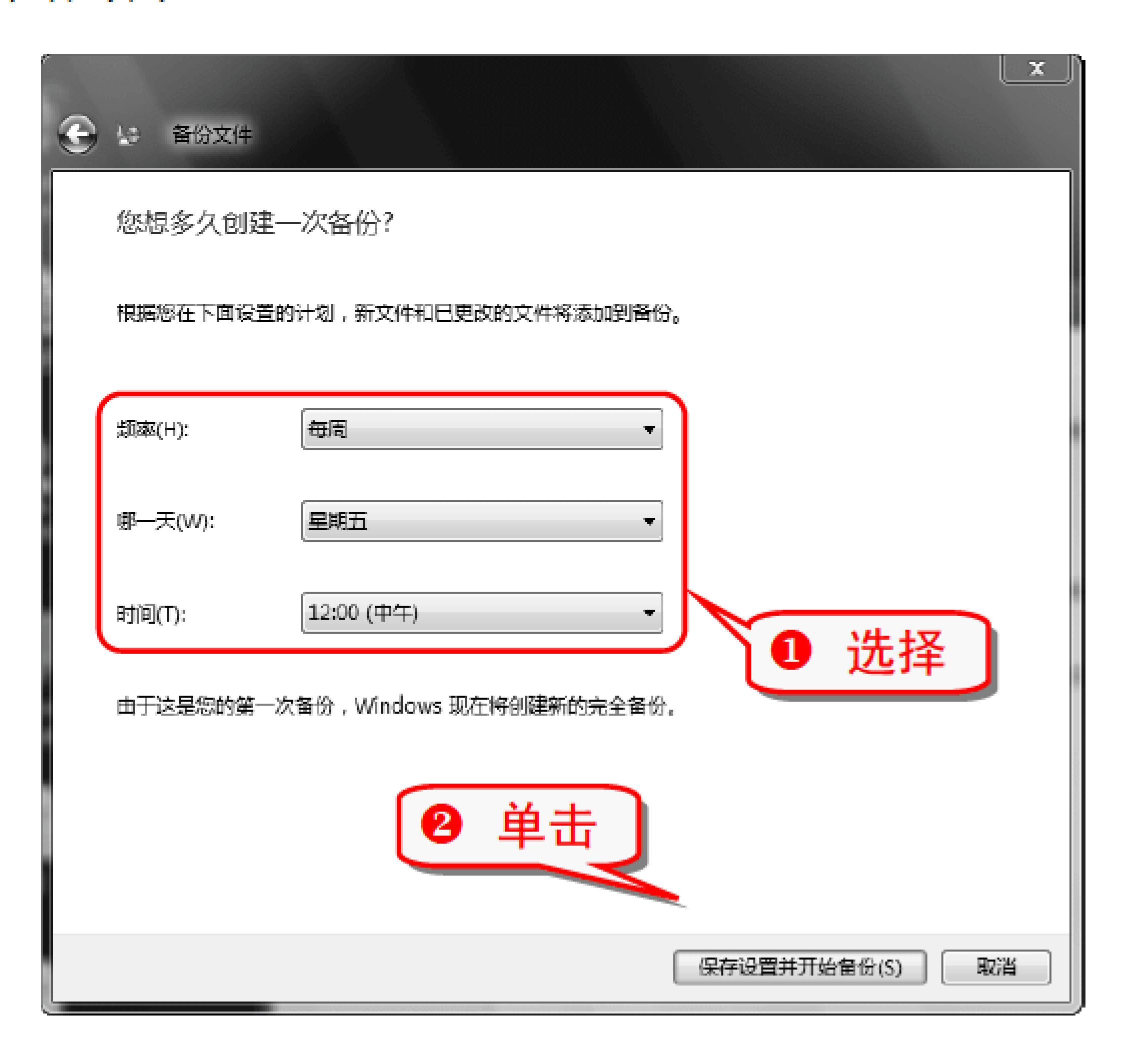
备份程序不能备份作为备份文件存放位置的盘，所以此处的 E 盘无法被备份，而系统盘将一直被默认备份。如果想备份 E 盘可在下一次备份的时候把备份文件存放位置选择为 D 盘。

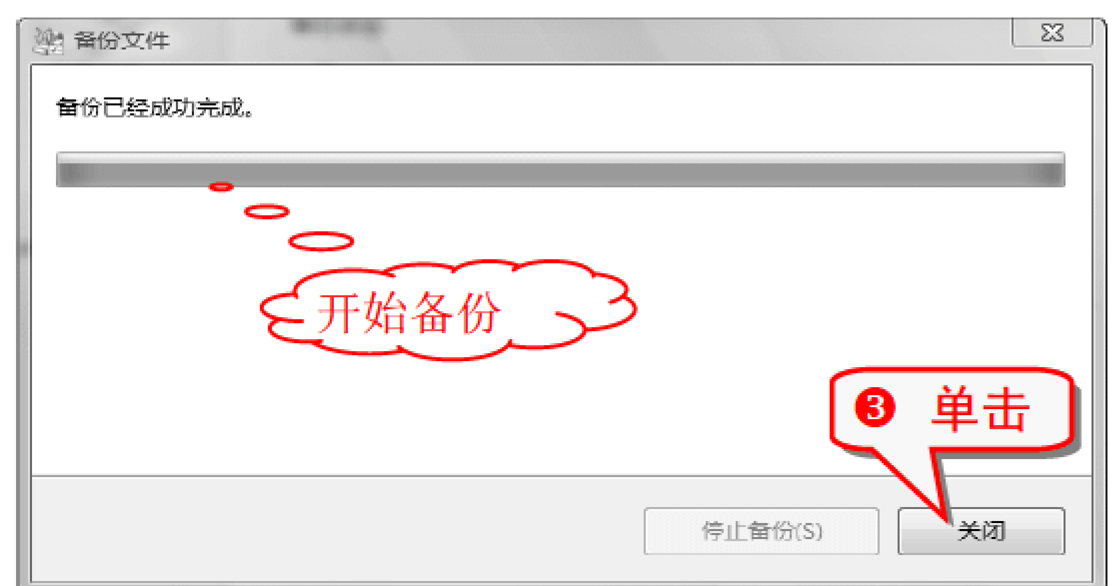


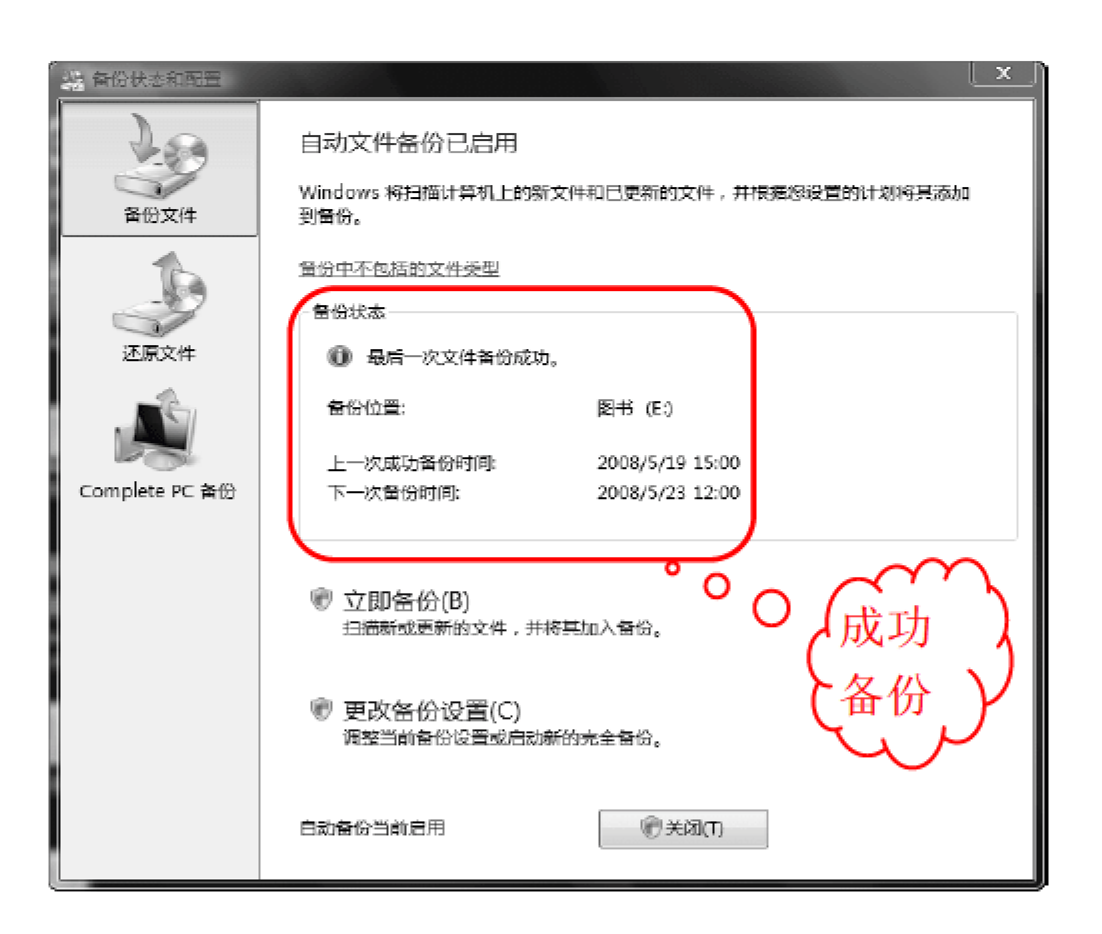


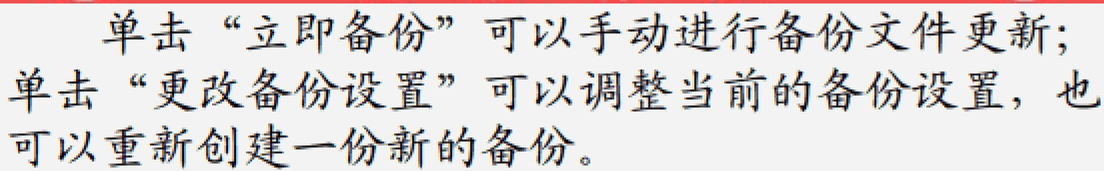
(2) 创建备份文件

用户根据个人情况设置备份频率、哪一天备份和备份详细时间。









单击“立即备份”可以手动进行备份文件更新；单击“更改备份设置”可以调整当前的备份设置，也可以重新创建一份新的备份。

技巧333　还原 Windows Vista 自动备份文件

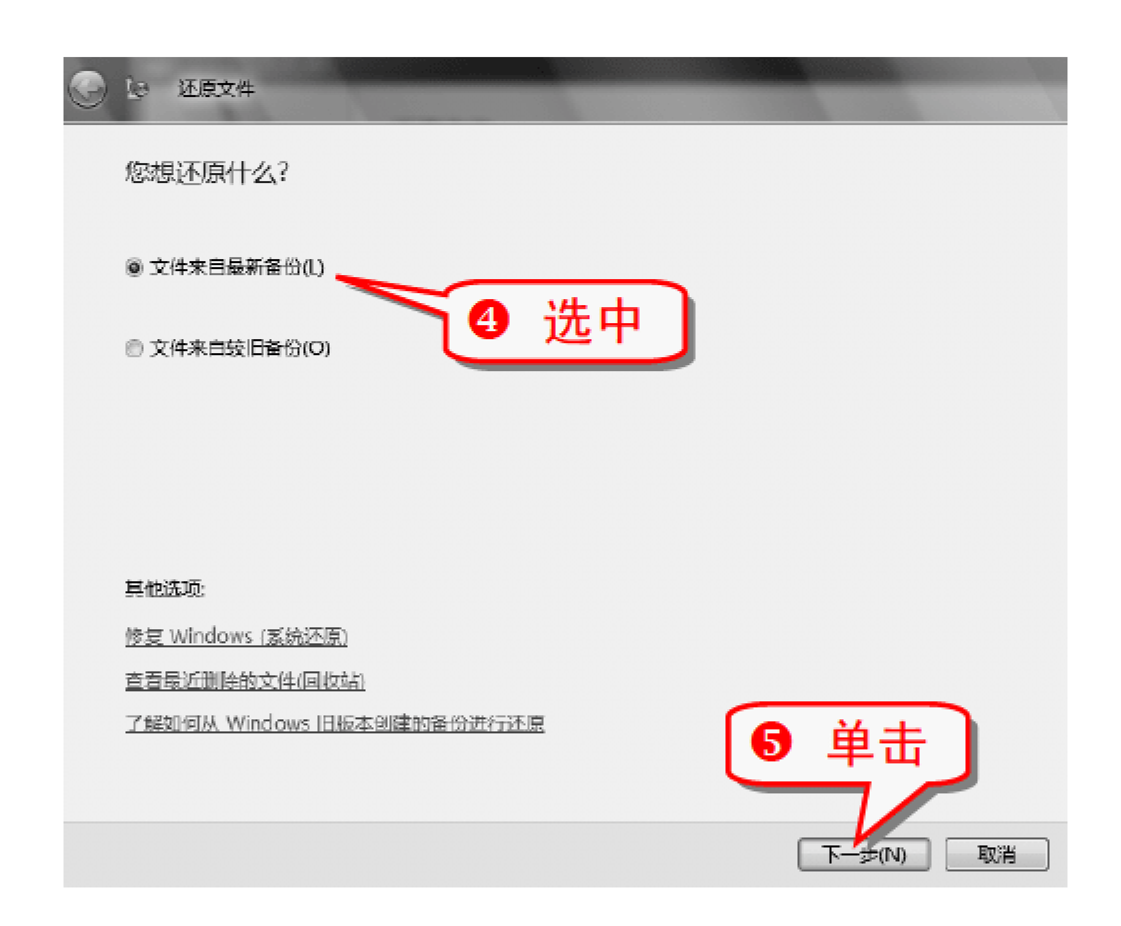
开启了 Windows Vista 系统自动文件备份功能后，用户可以随时将备份的文件进行还原。

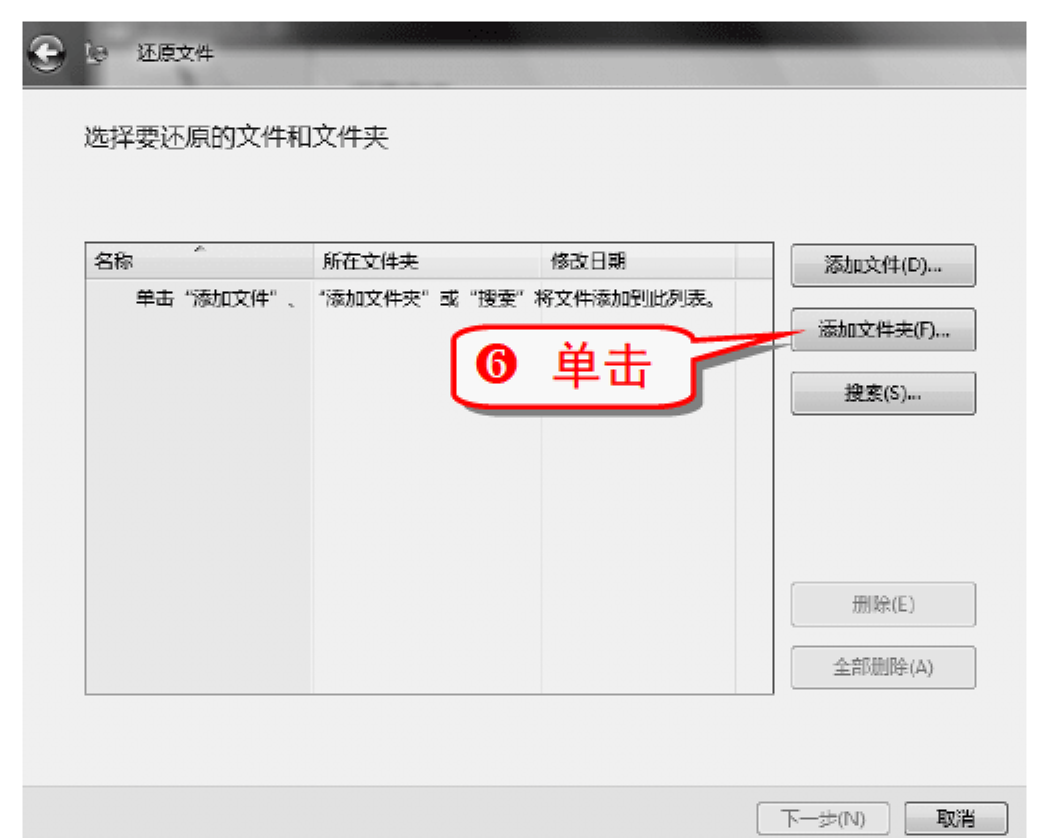
❶ 打开「开始」菜单，选择“所有程序”→“附件”→“系统工具”→“备份状态和设置”命令。



知　识　补　充

“高级还原”功能可以还原其他电脑或者此台电脑上所有用户的备份文件；而“还原文件”功能只可以还原此台电脑上的备份文件。





举 一 反 三

“添加文件”功能只可以还原单个文件；“添加文件夹”功能只可以还原整个文件夹；“搜索”功能可以快速搜索到相关可还原文件或者文件夹信息。





举 一 反 三

用户可以继续添加需要还原的文件或者文件夹，如果不需要还原某项文件或者文件夹，可先选中相应内容，再单击“删除”按钮。



注 意 事 项

选择“在原始位置”还原的时候，如果之前的文件没有被删除而且没有更改文件名，系统会弹出是否复制或者替换的提醒。选择“在以下位置”下拉列表，可以选择在源文件所在之外的其他位置进行还原。

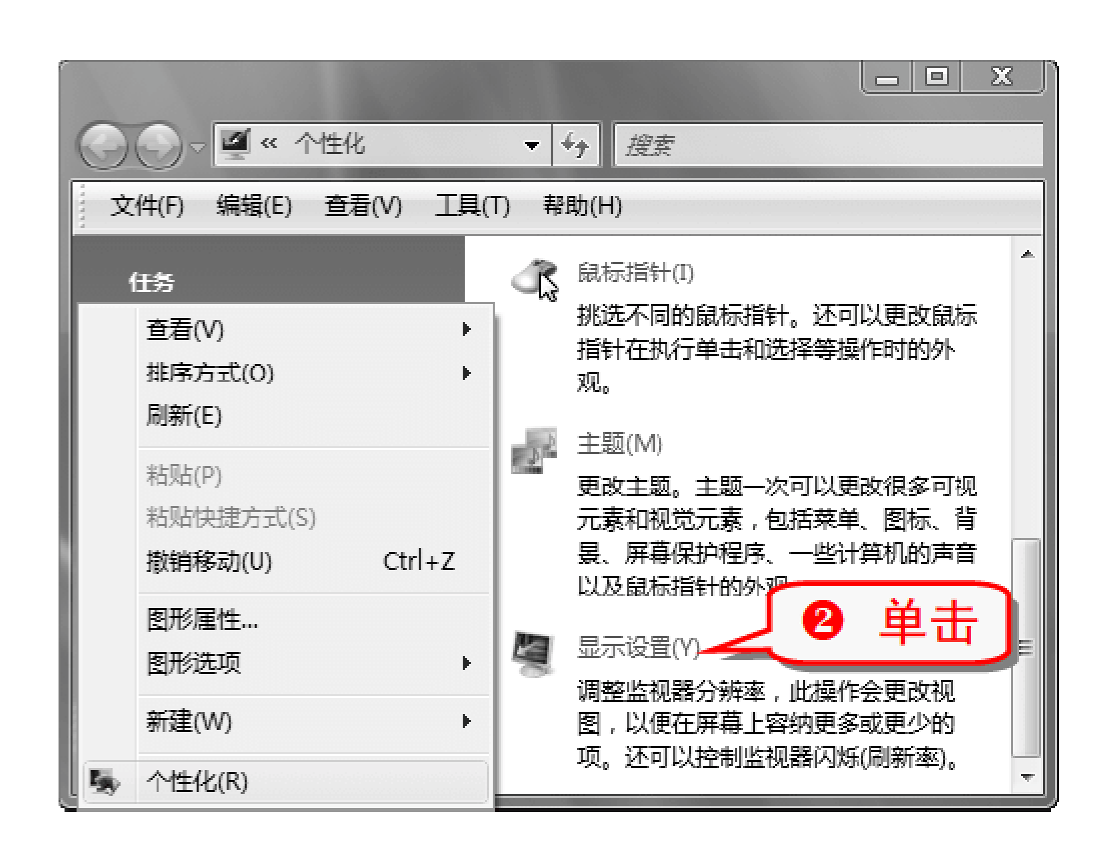
技巧334　查看驱动程序是否正确安装

没有安装或者错误地安装硬件的驱动程序，将导致系统不能很好地发挥其效用，也影响用户的使用。

如果显卡驱动没有安装好，将出现显示器画面低劣、屏幕闪烁的现象，用户眼睛极易疲劳。可以通过如下步骤查看其是否正确安装。

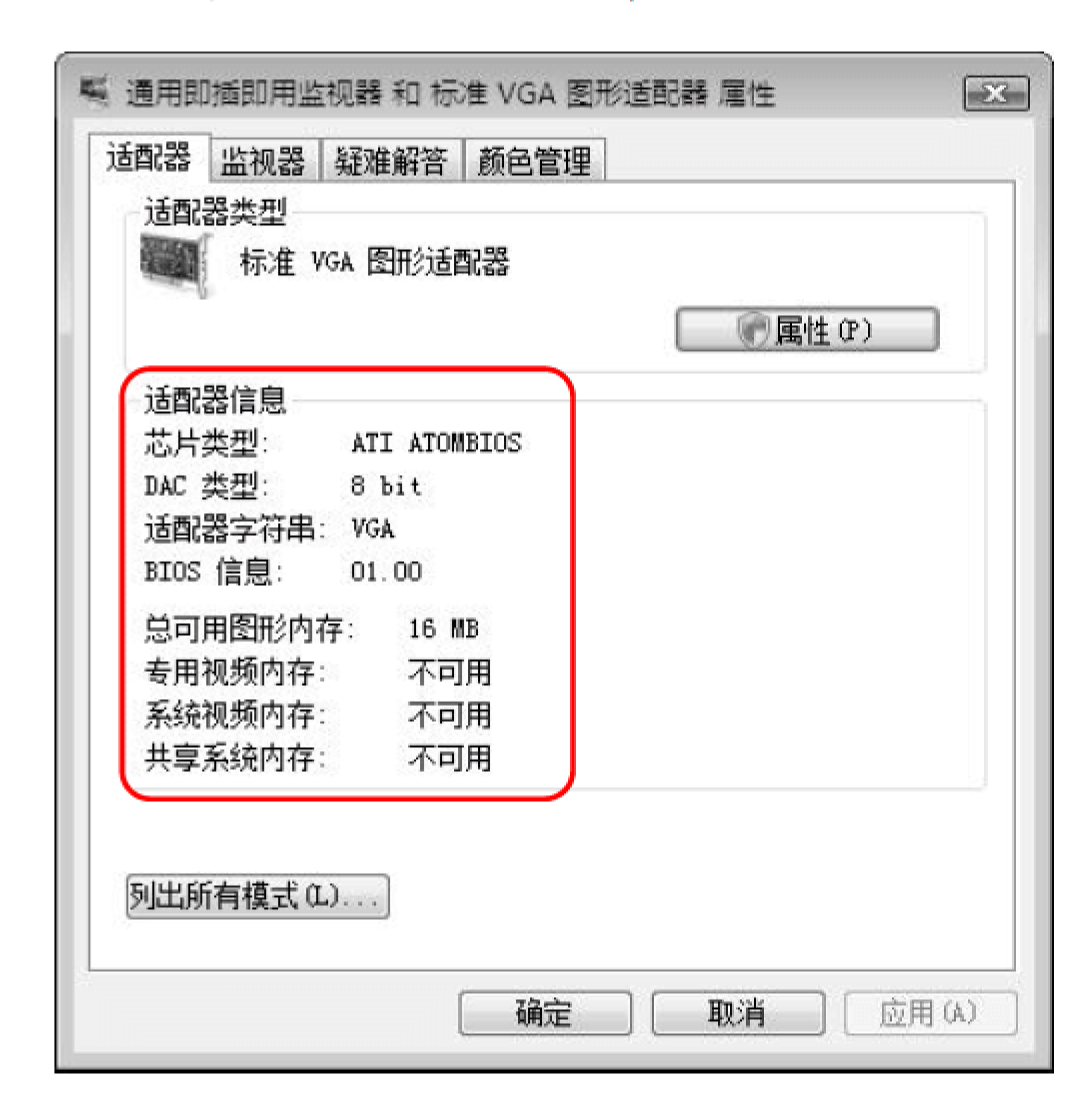
❶ 可以在桌面的任意位置右击，在弹出的快捷菜单中选择“个性化”命令，打开“个性化”窗口。



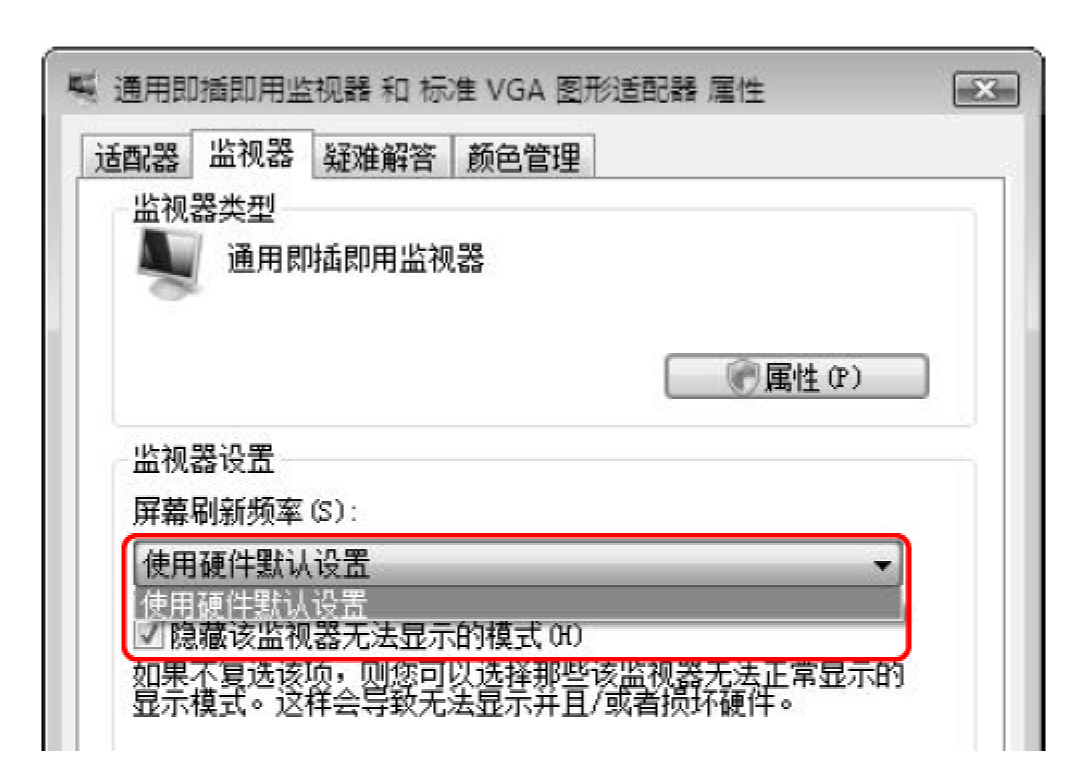




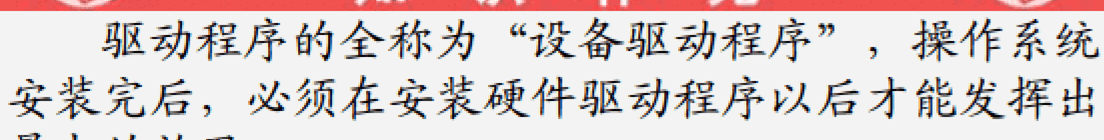
❹ 适配器和 BIOS 信息无法正常显示。



❺ 无法调整屏幕刷新频率。



❻ 可以判断其显卡驱动没有正确安装。



驱动程序的全称为“设备驱动程序”，操作系统安装完后，必须在安装硬件驱动程序以后才能发挥出最大的效用。

硬件驱动程序的安装方法目前主要有两种：一是运行硬件驱动程序的安装程序进行自动安装，称为“自动安装法”；另一种方式是手动添加驱动程序，称为“手工安装法”。

安装操作系统时，会自动安装大多数硬件设备的驱动程序，这些硬件设备的驱动程序都已经通过 WMD 的认证，并且可以在系统文件夹的 inf 目录下找到相应的硬件信息。

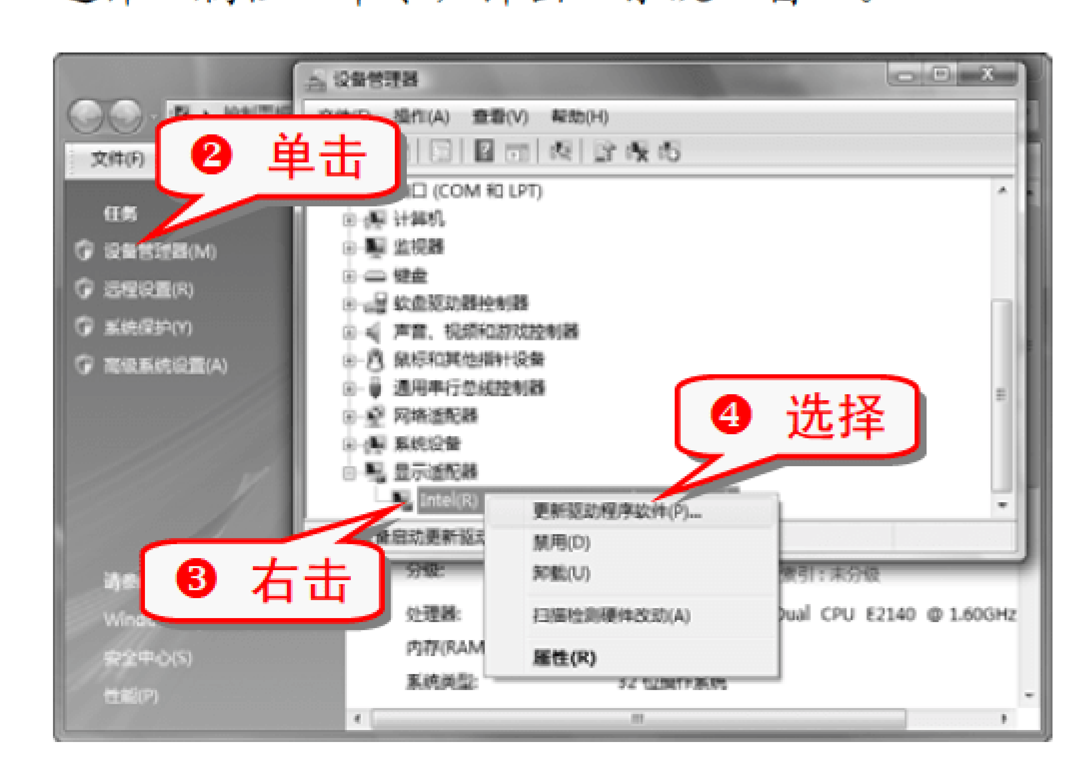
有的硬件驱动程序没有提供可执行的安装文件，此时就只能用“手工安装法”进行安装了。用“手工安装法”安装驱动程序比较麻烦，但不会安装附加软件，可以节约磁盘空间。

一般的安装顺序为主板驱动程序、显卡驱动程序、声卡驱动程序以及网卡驱动程序等。

技巧335　手动更新驱动程序

对于显卡驱动没有正确安装的情况，可以通过更新显卡驱动或者重新安装显卡驱动来解决。

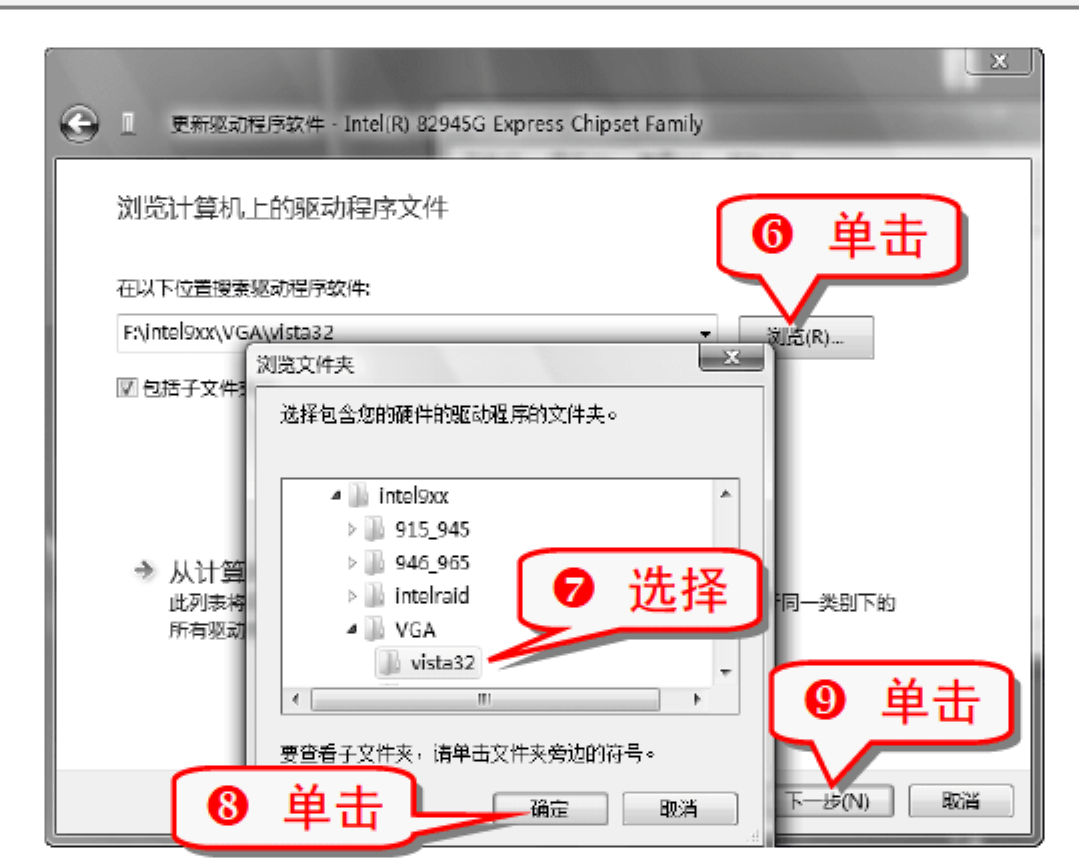
❶ 右击桌面上的“计算机”图标，在弹出的快捷菜单中选择“属性”命令，弹出“系统”窗口。





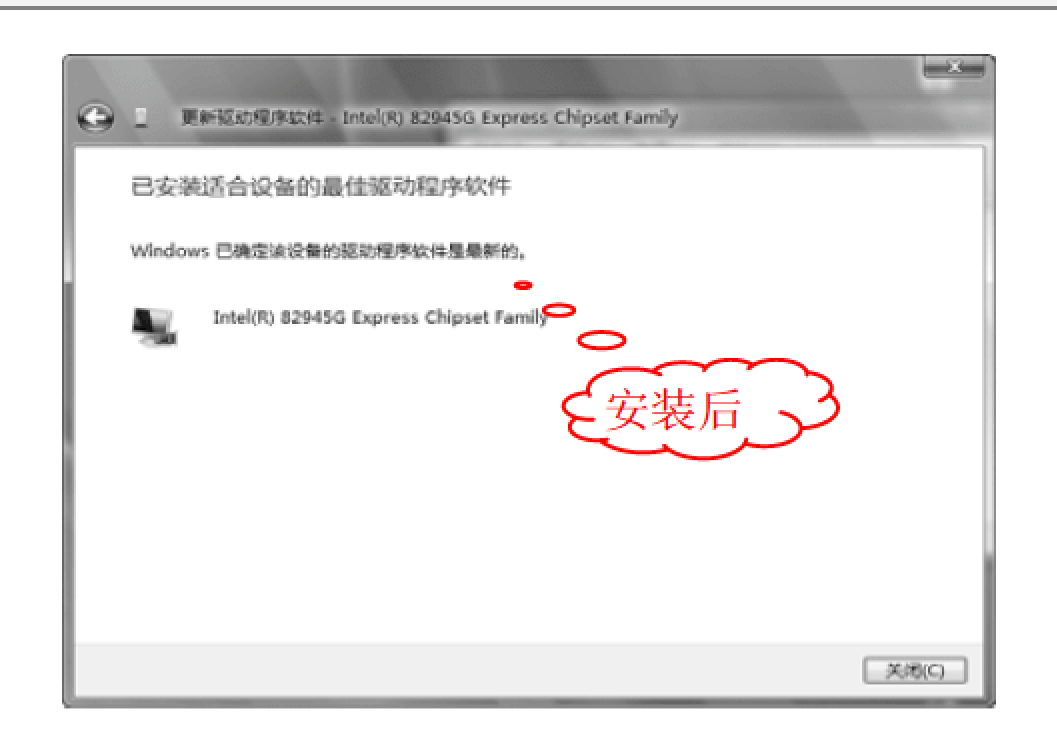
知 识 补 充

选择“自动搜索更新的驱动程序软件”，系统将自动搜索本地计算机和 Internet 上相关的最新驱动程序。



专 家 坐 堂

显卡、声卡以及网卡的驱动程序都保存在 C:\Windows\System32\Drivers 目录下，有时候系统出现故障会导致无法识别网卡等硬件，可以尝试将自动搜索目录设置到上述位置更新驱动。



技巧336　手动备份驱动程序

及时备份驱动程序可以让系统的重装有备无患，Windows 系统下驱动程序的安装路径为系统盘 Windows 目录下的 inf、System 和 System32 三个文件夹。

完成驱动程序安装后，将这三个文件夹复制到非系统盘上做备份。重装系统时只需将其覆盖回 Windows 目录下即可。

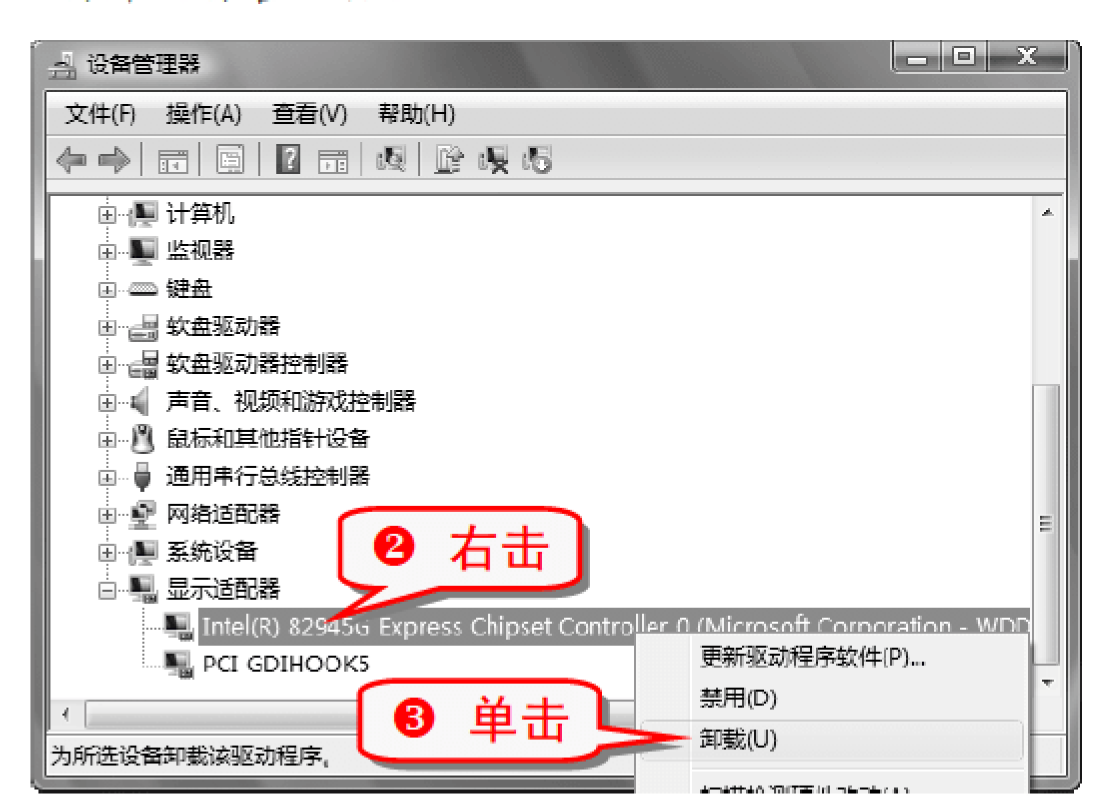
技巧337　手动卸载驱动程序

如果现有的驱动程序版本功能或者性能不够完善，可以通过安装新的驱动程序来升级；如果原先驱动安装有问题，或者使用时被破坏了，可以通过原来的驱动程序修复安装。

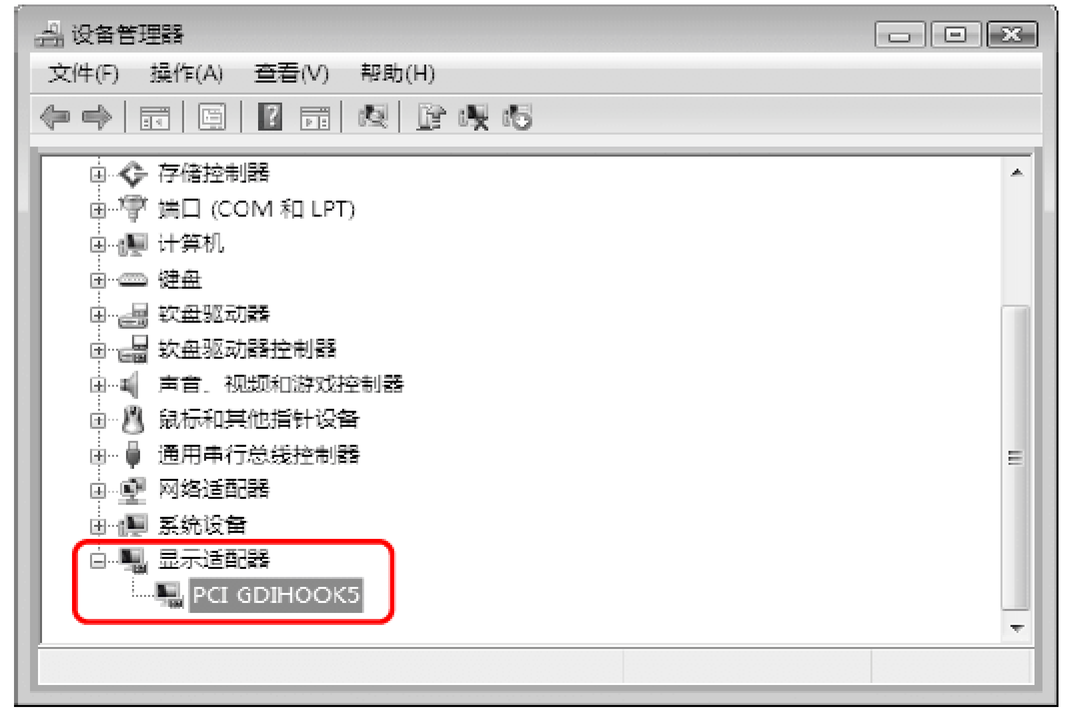
当安装新版本的驱动程序后系统变得不够稳定时，则需要将现有的驱动程序卸载后安装老版本驱动程序。

(1) 在“设备管理器”中卸载驱动程序

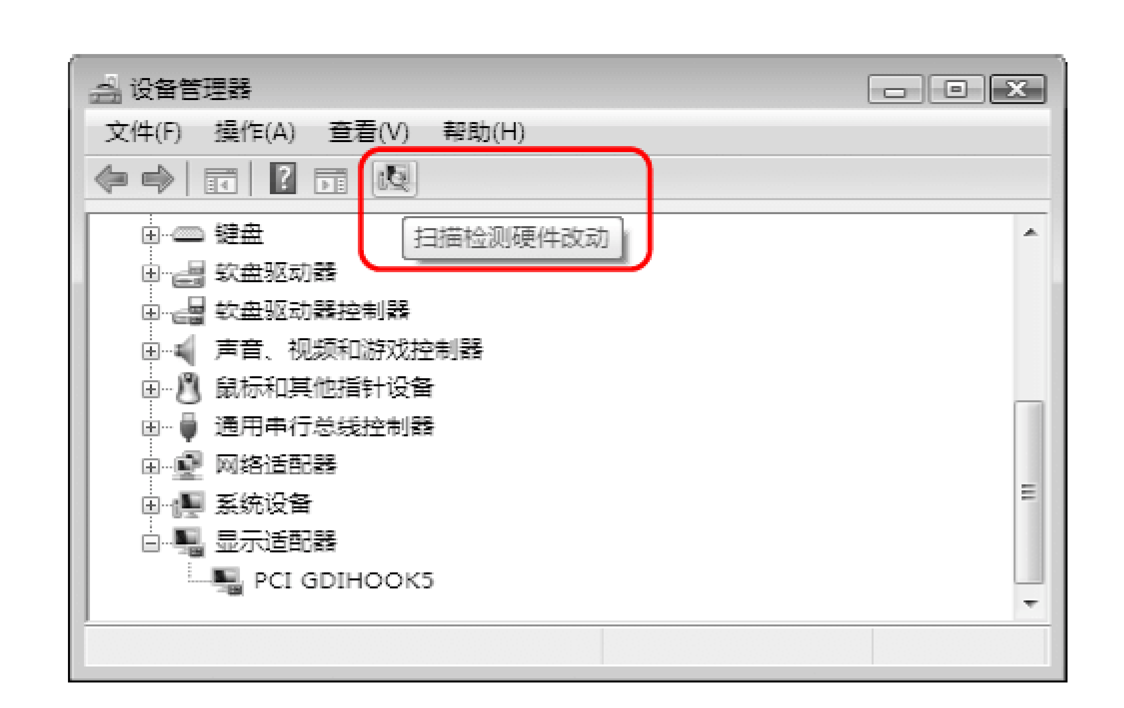
❶ 打开设备管理器。









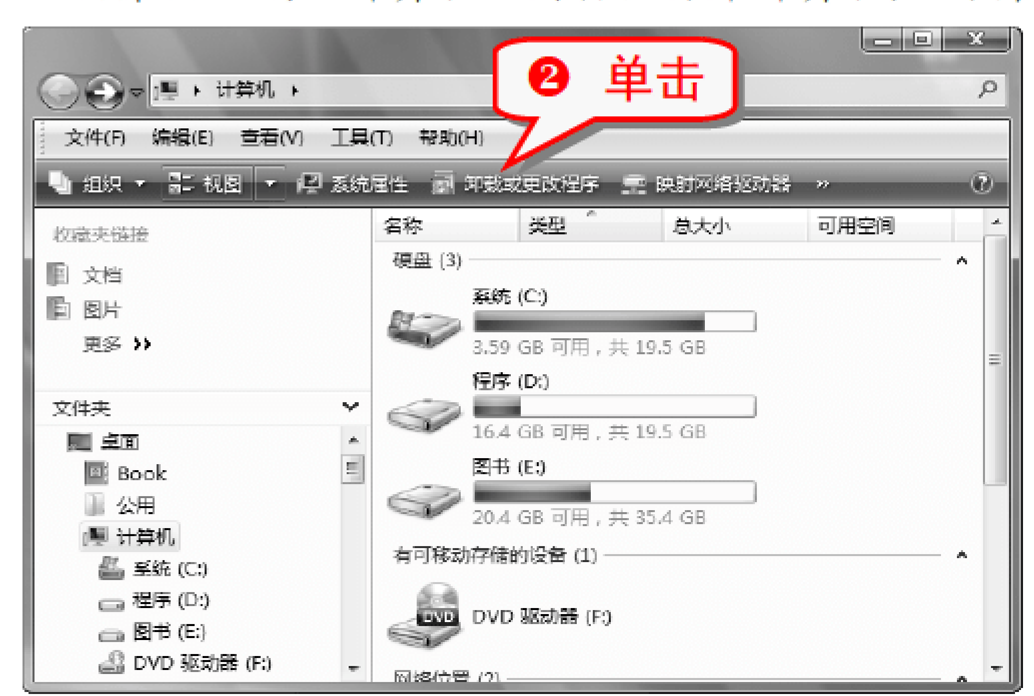


注　意　事　项

使用上述方法卸载的驱动程序，可以通过按钮扫描检测硬件改动来找回。

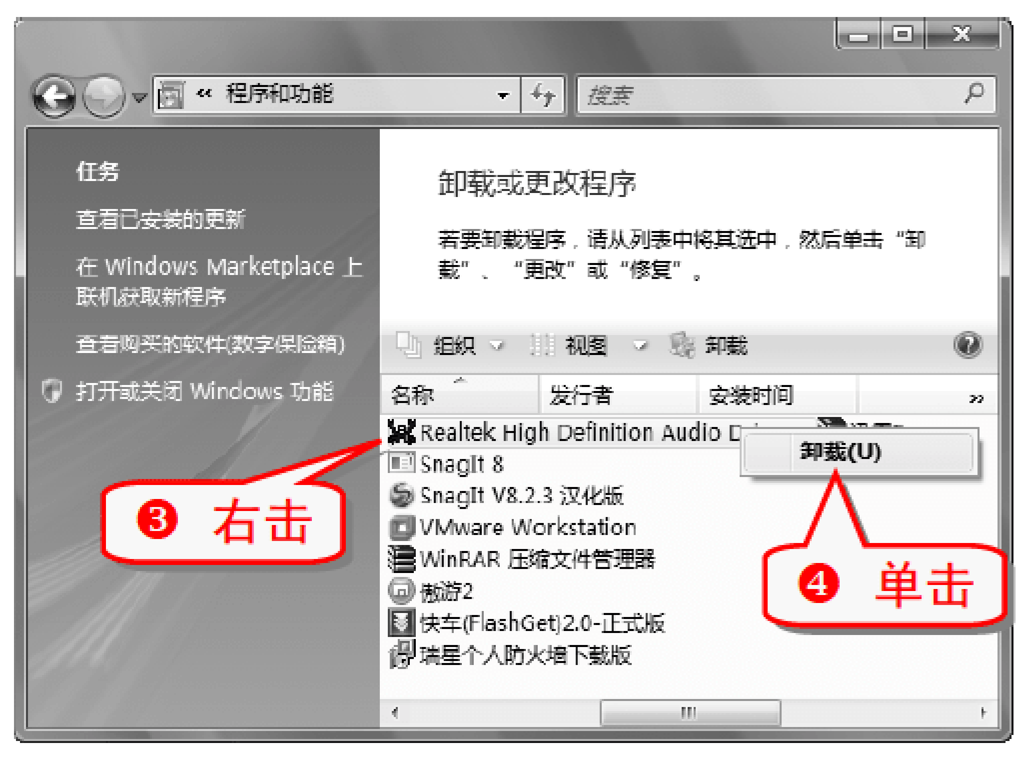
(2) 在“卸载或更改程序”中卸载驱动程序

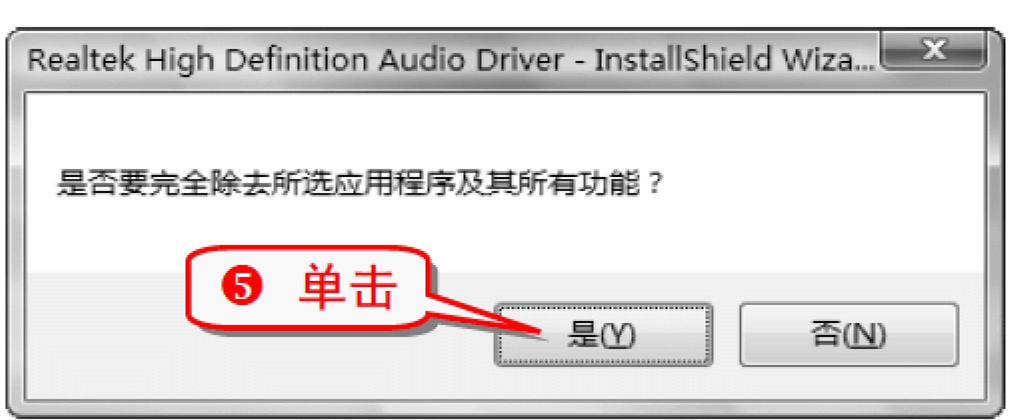
❶ 双击桌面上的“计算机”图标，打开计算机应用窗口。



举　一　反　三

用户也可以依次单击“控制面板”→“程序”→“程序和功能”命令，打开“卸载或更改程序”界面。







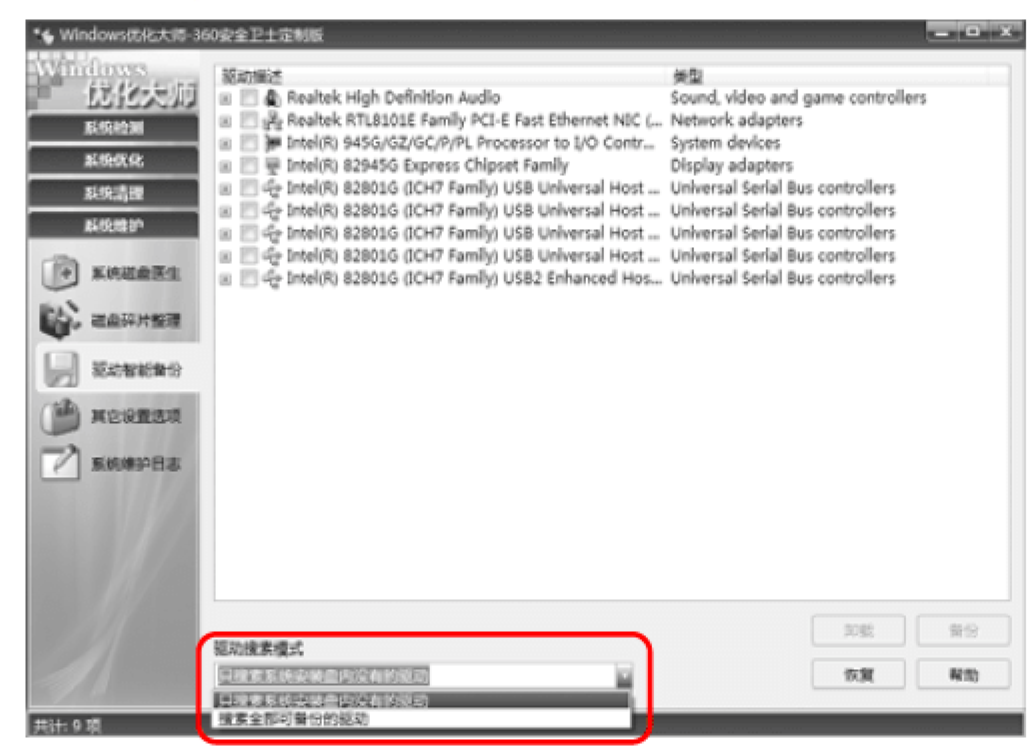


技巧338　使用 Windows 优化大师备份驱动程序

手动备份驱动程序，操作相对比较繁琐，使用工具软件备份可以更为便捷。

Windows 优化大师是一款功能强大且操作简便的系统辅助软件，可以方便地备份和还原驱动程序。

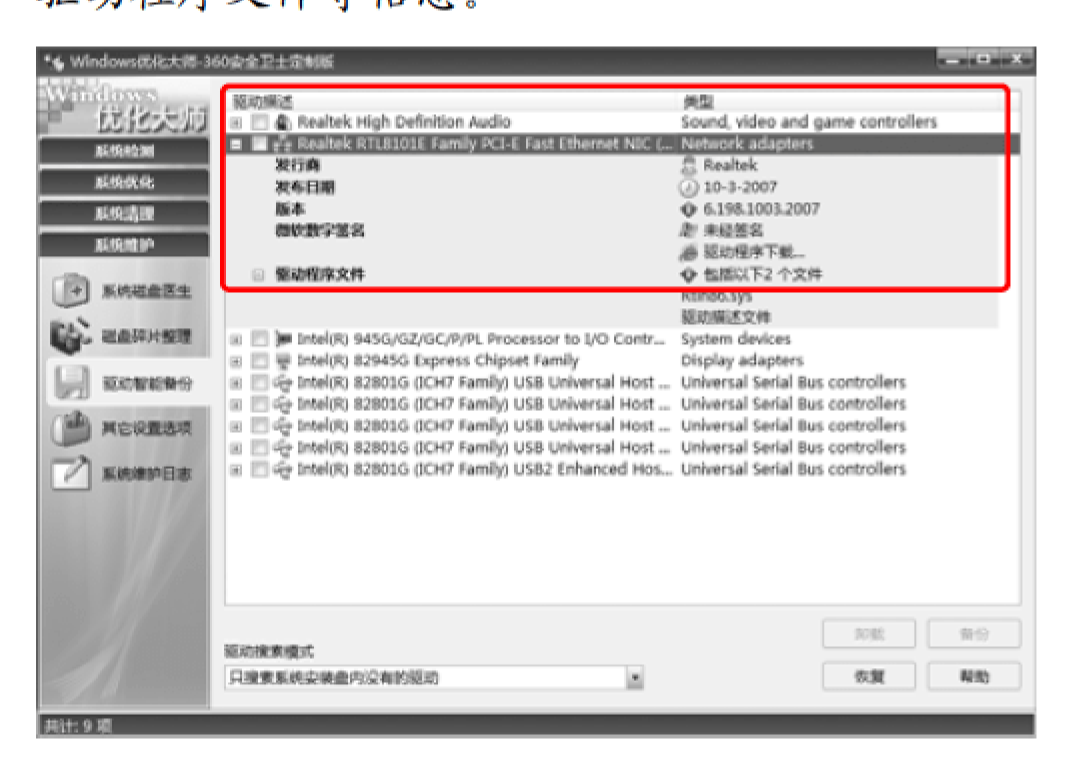
❶ 打开 windows 优化大师，选择“系统维护”选项下的“驱动智能备份”选项。



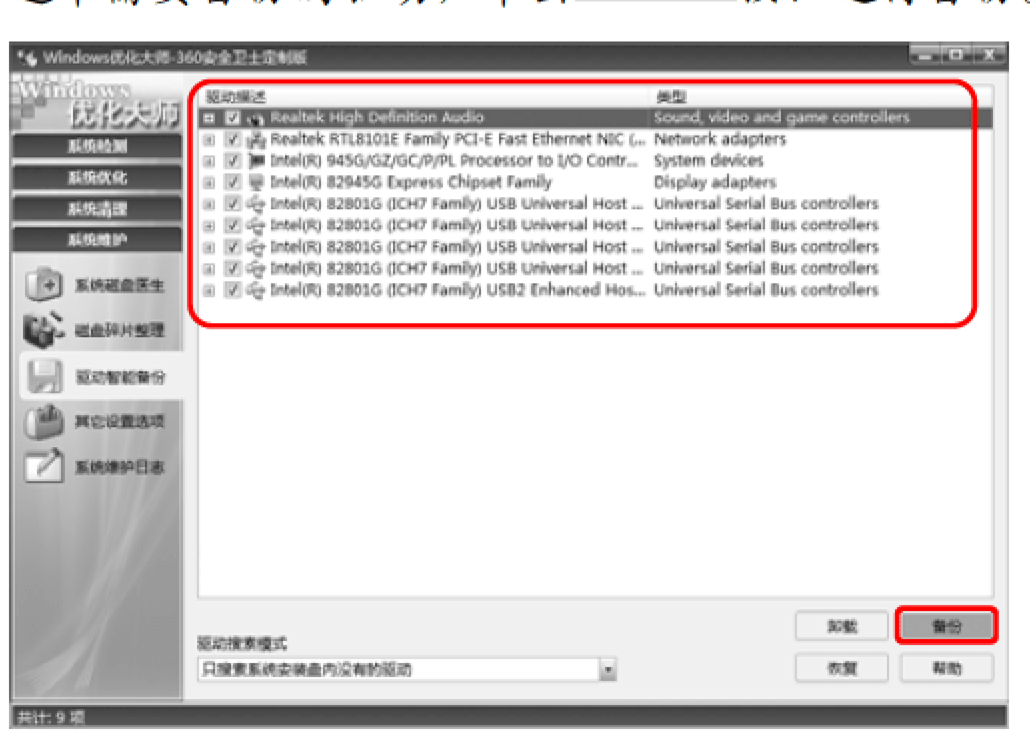
知　识　补　充

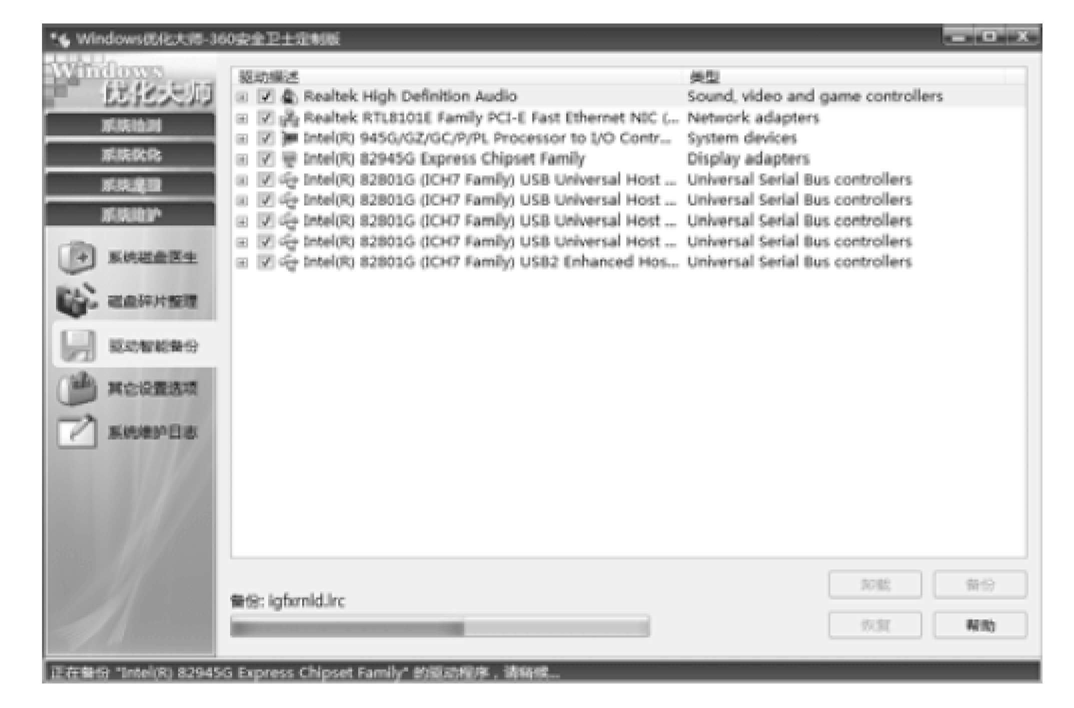
“驱动搜索模式”下拉列表默认列出的驱动程序均为系统安装盘所没有的驱动程序，如果需要完整备份请选择“搜索全部可备份的驱动”选项。

❷ 单击驱动前的 ⊞ 图标，可以显示该驱动的详细信息。包括：发行商、发行日期、版本、微软数字签名以及驱动程序文件等信息。



❸ 选中需要备份的驱动，单击 备份 按钮进行备份。

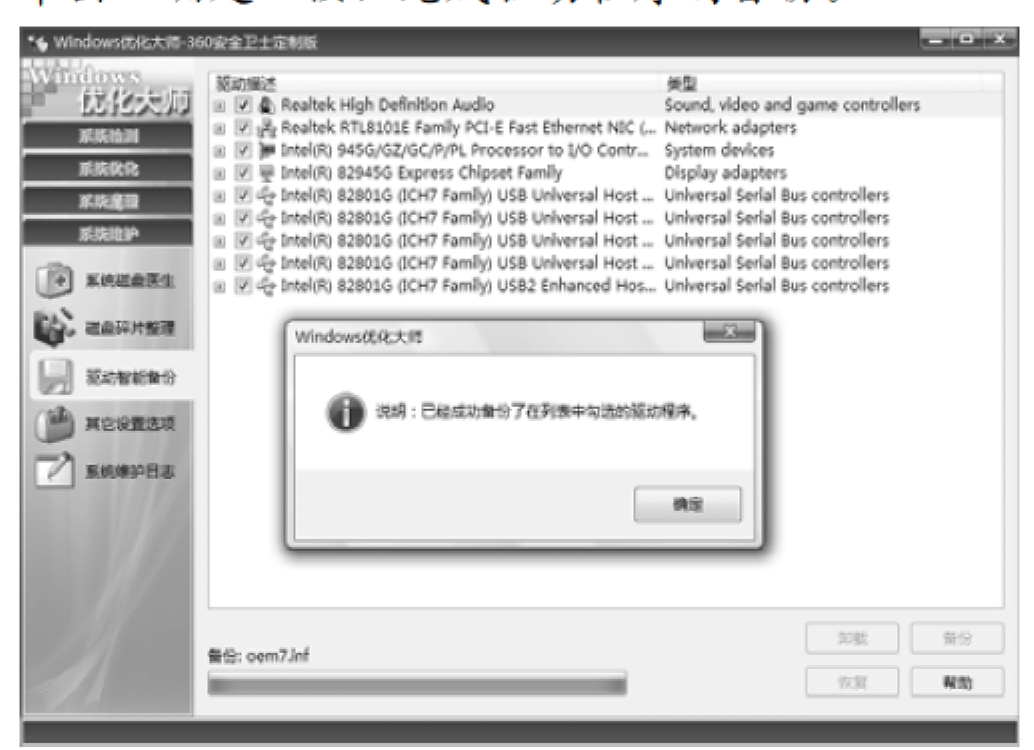




❹ 如果 Windows 优化大师在备份时候检查到该驱动已经进行过备份，会提示用户是否还要备份，若不需要重复备份，单击“取消”按钮即可。



❺ 单击“确定”按钮完成驱动程序的备份。

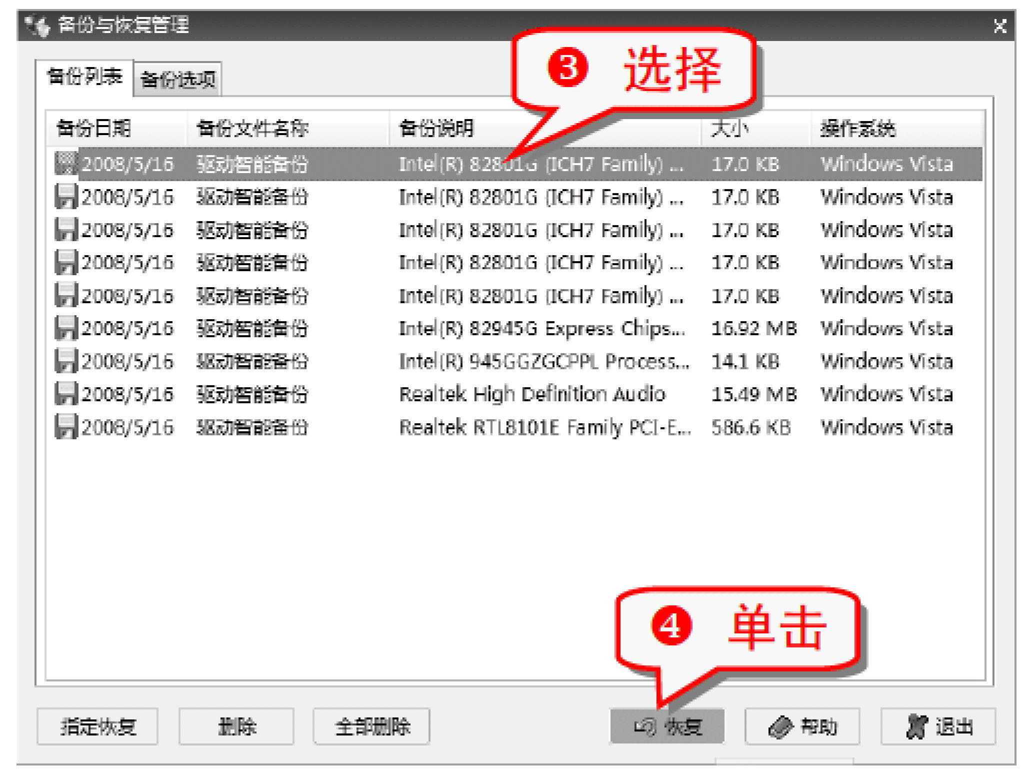


技巧339 使用 Windows 优化大师恢复驱动程序

完成备份后，只要没有删除备份文件，就可以随时通过 Windows 优化大师恢复驱动程序。

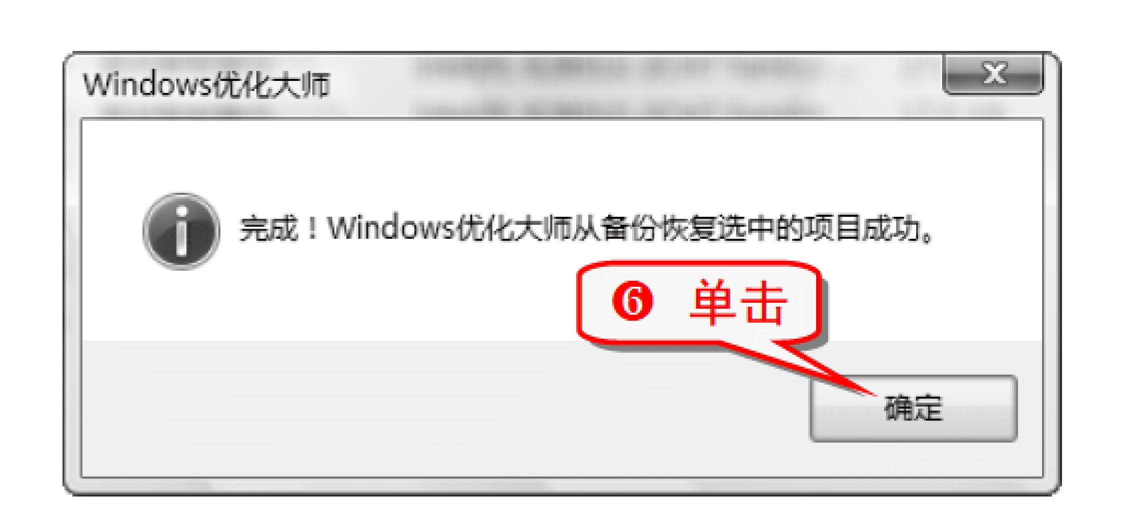
❶ 打开 Windows 优化大师。











举 一 反 三

手工安装驱动程序时，也可以让 Windows 到 Windows 优化大师的驱动备份目录去寻找驱动。

❼ 在“备份与恢复管理”窗口中可以设置备份时选用的压缩率以及备份文件保存的目录。



技巧340　使用驱动精灵更新驱动程序

驱动精灵是一款由业内知名专业站点——驱动之家(Mydrivers.com)推出的驱动程序专业应用工具软件。

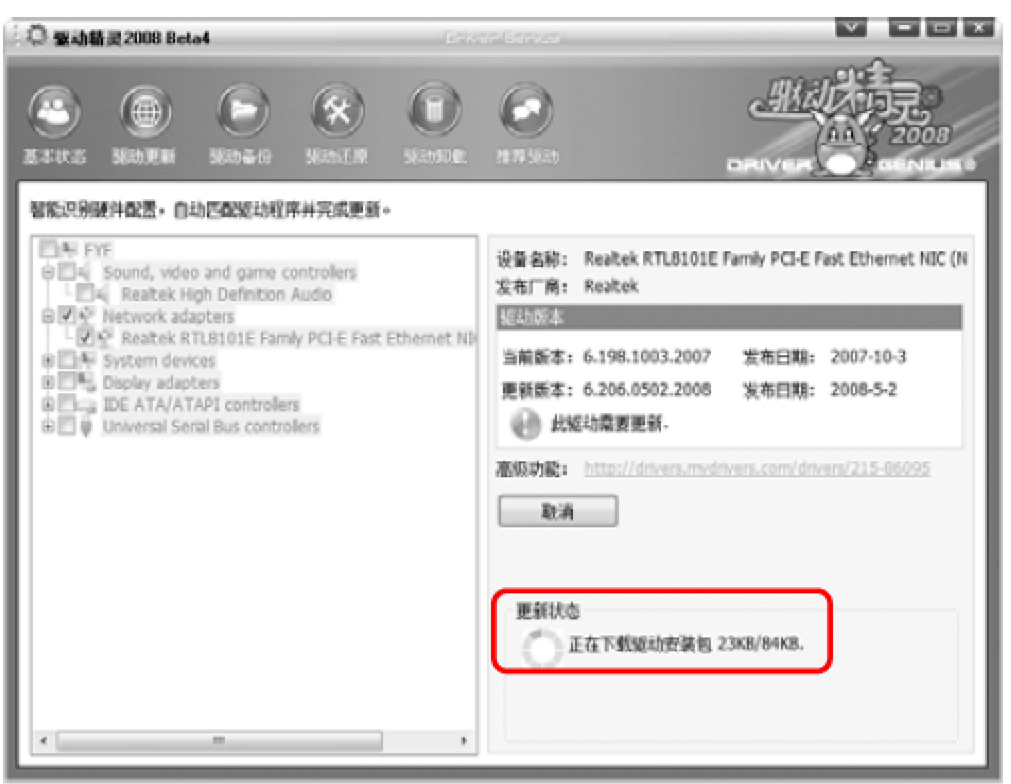
驱动精灵采用先进的硬件检测技术，不仅可以替未知设备安装驱动程序，还能自动检测驱动升级，让电脑保持最佳工作状态。其备份和还原操作也非常方便。

❶ 启动驱动精灵，打开如下界面。



❸ 驱动精灵会智能识别本机的硬件设备，列出所选的驱动的详细信息以及是否需要更新。







注 意 事 项

可以在将全部驱动更新之后再重新启动电脑，避免频繁重新启动对电脑造成伤害。

技巧341　使用驱动精灵备份驱动程序

驱动精灵可以将硬件驱动程序备份为独立的文件、Zip 压缩包、自解压程序或自动安装程序。

❶ 启动驱动精灵，打开如下界面。

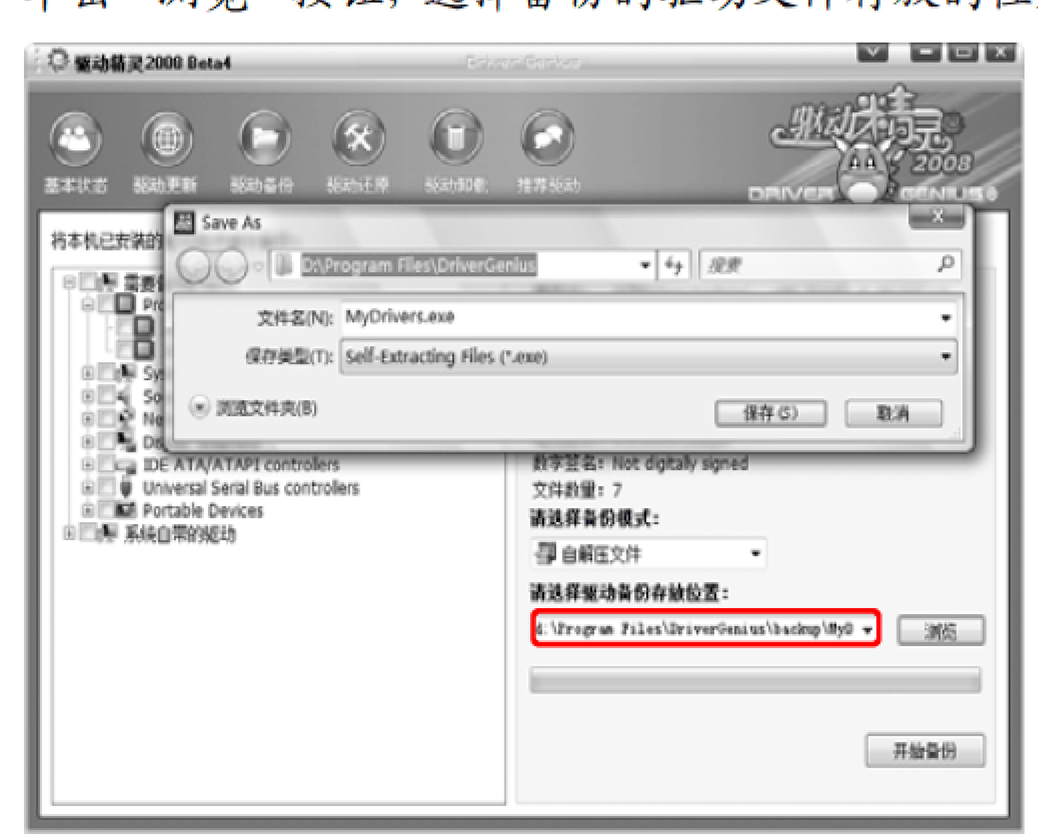




❸ 选择备份的模式：ZIP 格式、文件夹或是自解压文件。



❹ 单击“浏览”按钮，选择备份的驱动文件存放的位置。







技巧342 使用驱动精灵还原驱动程序

驱动精灵的还原功能非常简单易用。

❶ 启动驱动精灵，打开如下界面。

















举　一　反　三



双击驱动精灵备份的自安装驱动程序即可一键完成硬件驱动程序的安装。

技巧343　使用驱动精灵删除驱动程序

驱动程序安装错误或者卸载不完全都有可能影响操作系统的稳定运行，使用驱动精灵的驱动卸载功能，可以安全卸载驱动程序以及清理操作系统中残留的驱动，将操作系统保持在最佳工作状态。

❶ 启动驱动精灵，打开如下界面。





注　意　事　项



某些硬件设备关系到系统的正常运行，请谨慎使用卸载功能。建议在卸载驱动前先备份驱动程序。



专题十三　备份与恢复私人数据

内容导航

对电脑系统数据进行备份很重要，对于私人的数据备份也很重要。做好私人数据的备份，能最大限度地减少个人数据的损坏或丢失。

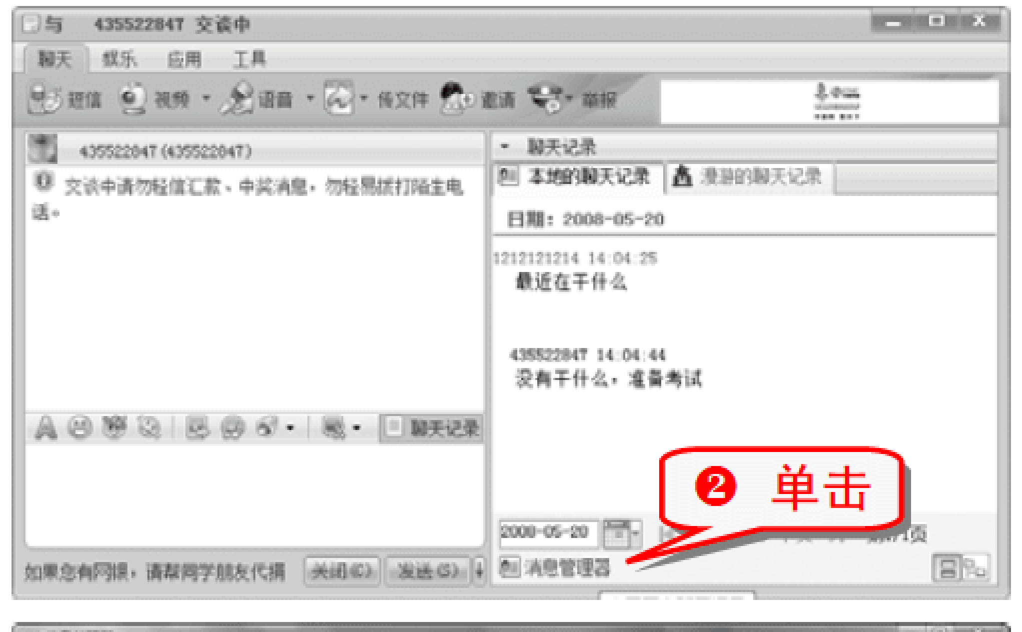
热点快报

- 备份 QQ 聊天记录
- 备份收藏夹
- 备份 QQ 表情
- 备份网络参数设置
- 备份 MSN 联系人
- 备份输入法

技巧344　备份特定好友的 QQ 聊天记录

QQ 的好友名单存储在腾讯服务器上，但是聊天记录和个人信息都是存放在本地硬盘上，重装系统或者误删除文件，都会导致 QQ 数据的丢失，所以有必要掌握备份 QQ 数据的方法。如果只需要备份 QQ 聊天记录，可以直接使用消息管理器来进行数据备份。

❶ 在 QQ 主界面上双击任一好友的头像，弹出对话窗口。









专家坐堂

“导出”菜单下有四个选项。其中，“导出聊天记录为文本文件”命令将导出一个以 TXT 为扩展名的备份文件，可直接双击查看，“导出聊天记录为备份文件”命令则导出扩展名为 BAK 的备份文件，不可以直接双击查看。

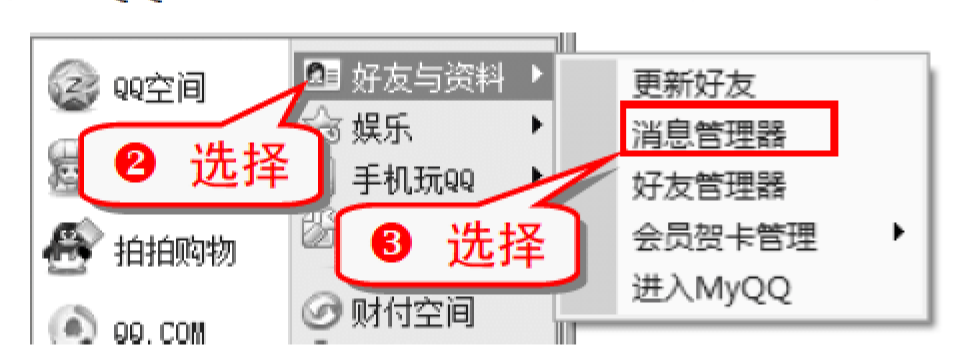
技巧345　备份与还原所有 QQ 聊天记录

可以将所有好友的聊天记录都备份下来。

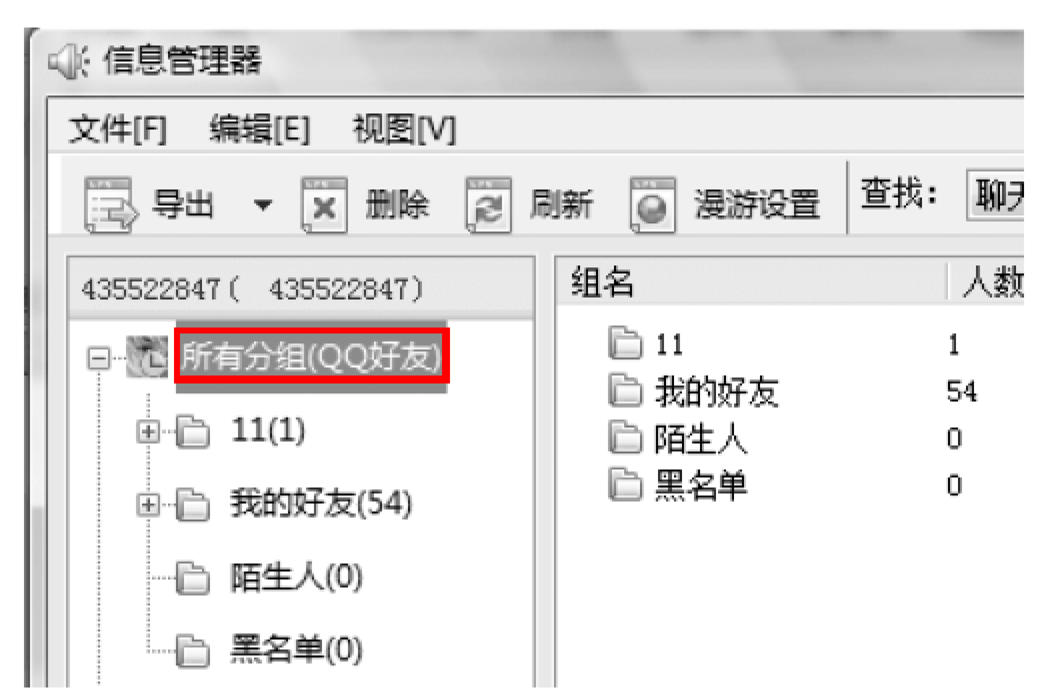
(1) 备份所有 QQ 聊天记录

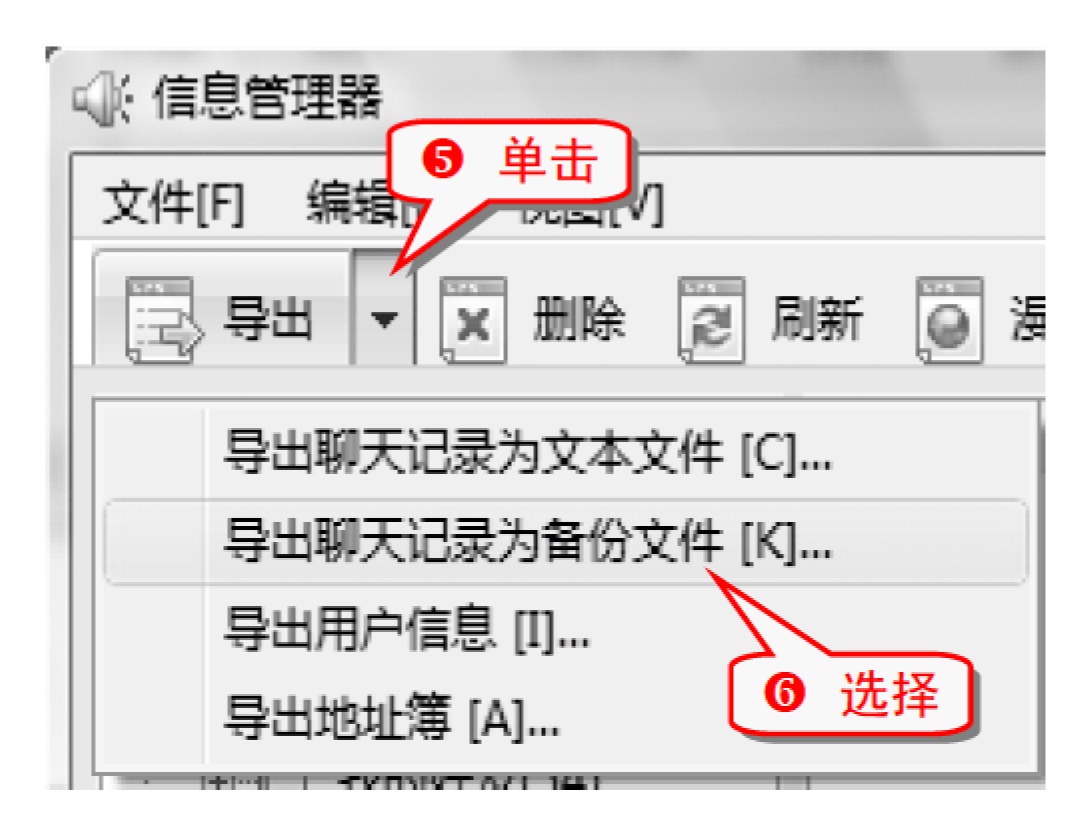
备份所有 QQ 聊天记录的方法非常简单方便。

❶ 单击 QQ 面板下方的图标，打开系统菜单。

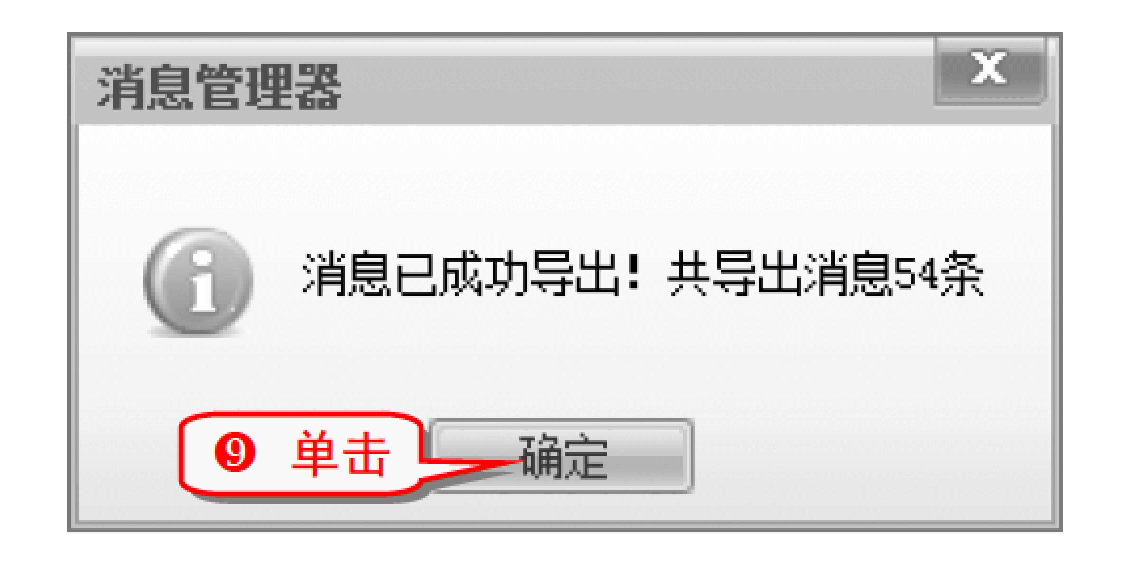


❹ 弹出“信息管理器”窗口，选择“所有分组”选项。



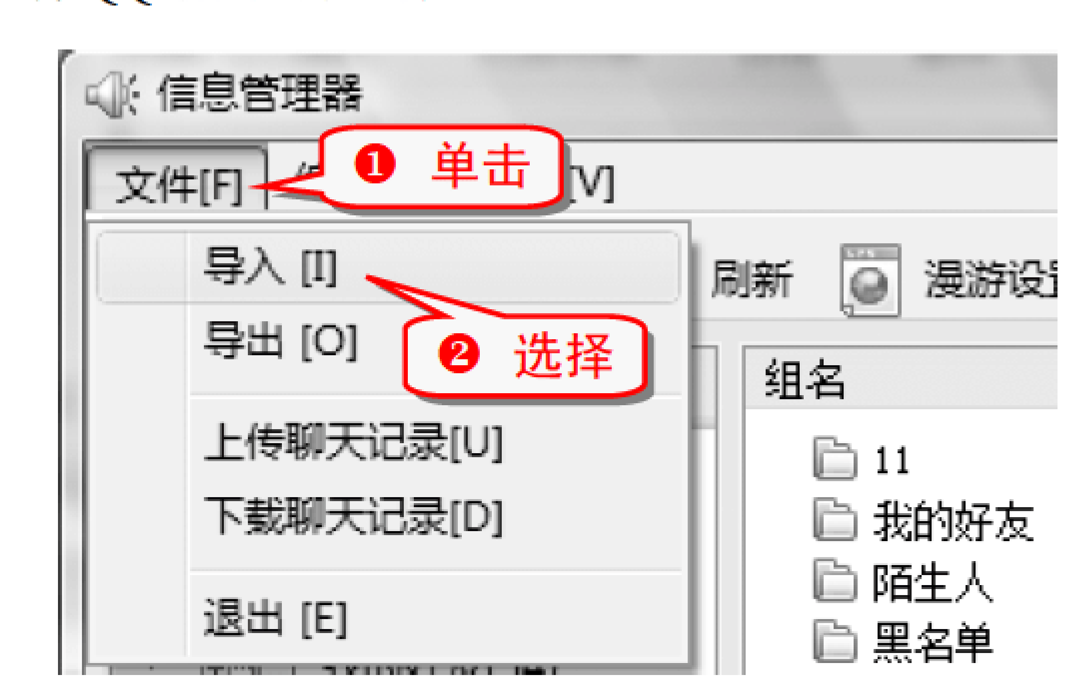


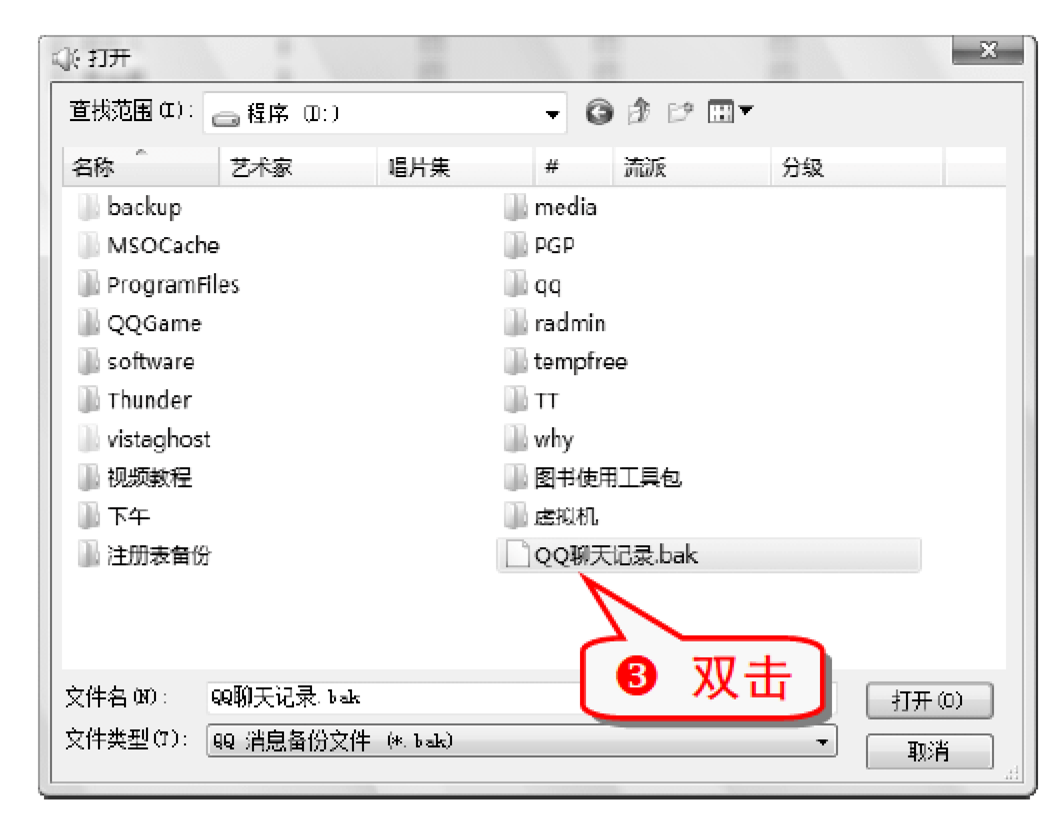


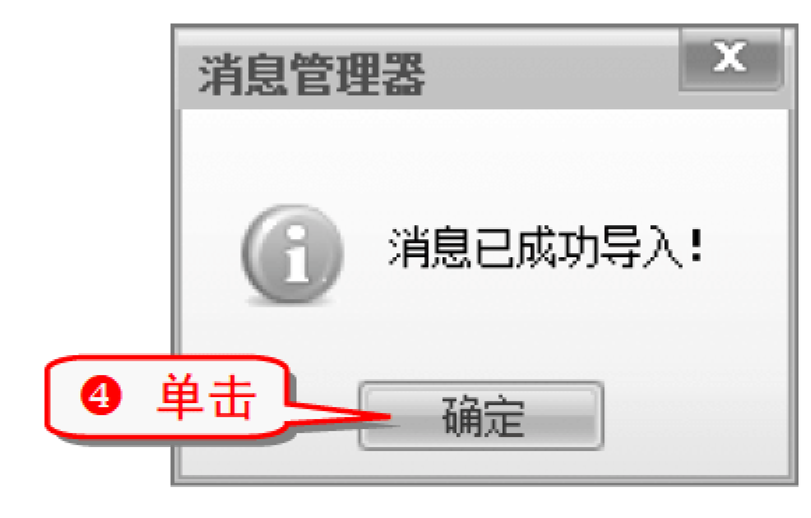


(2) 还原 QQ 聊天记录

将 QQ 聊天记录导出为备份文件后，利用其导入功能可将 QQ 聊天记录还原。







技巧346　备份和还原 QQ 表情

在聊天的时候利用 QQ 的自定义添加表情的功能，使自己的聊天变得生动。但是重装 QQ 后就会丢失精心收藏的 QQ 表情，重新收集 QQ 表情又很耗时。如果将 QQ 表

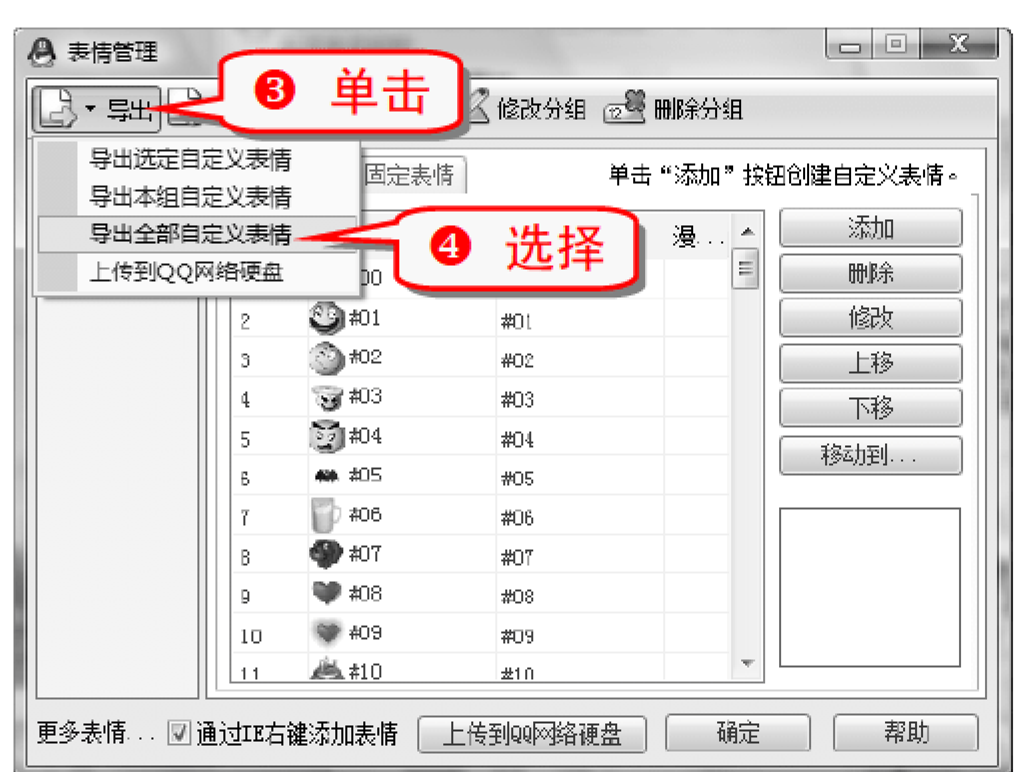


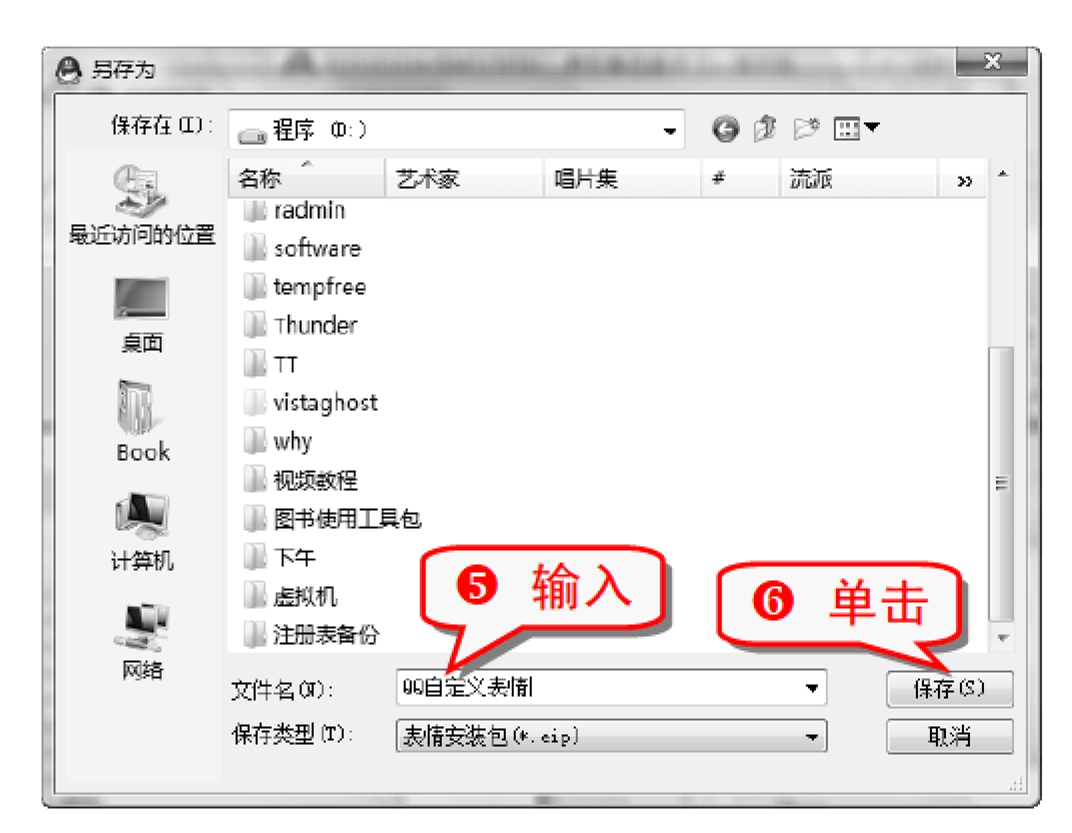
情备份了，就不会出现这样的问题。

(1) 备份 QQ 表情

❶ 打开一个 QQ 聊天窗口，单击聊天面板上的😀图标。



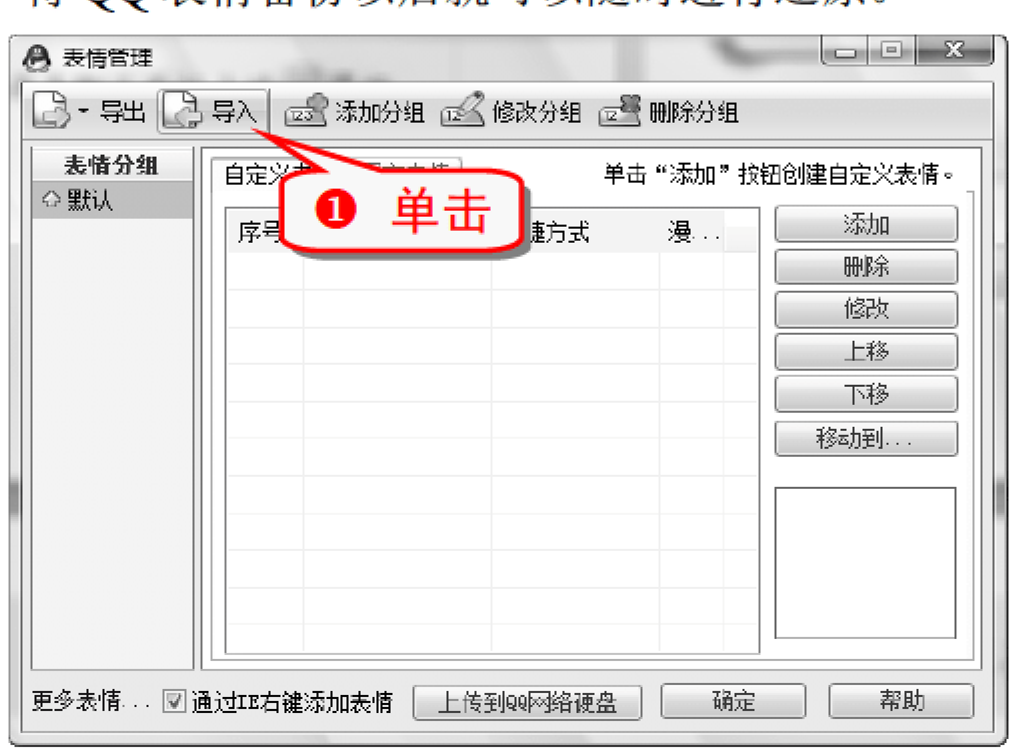


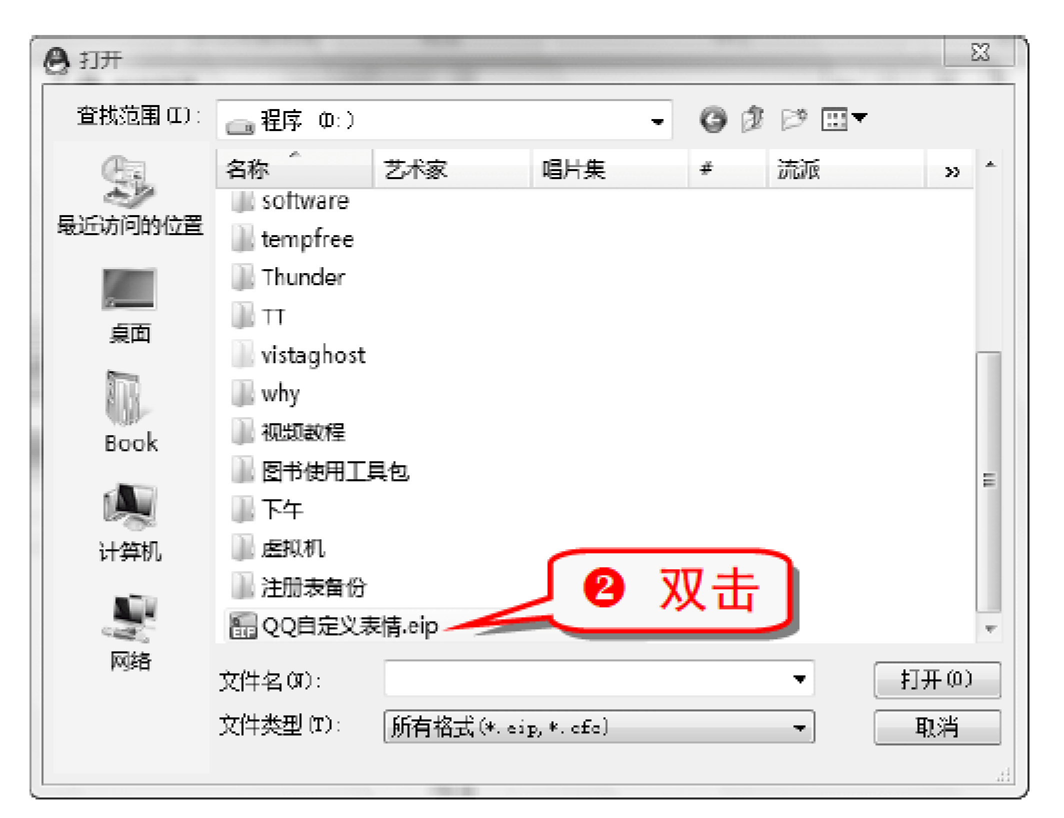


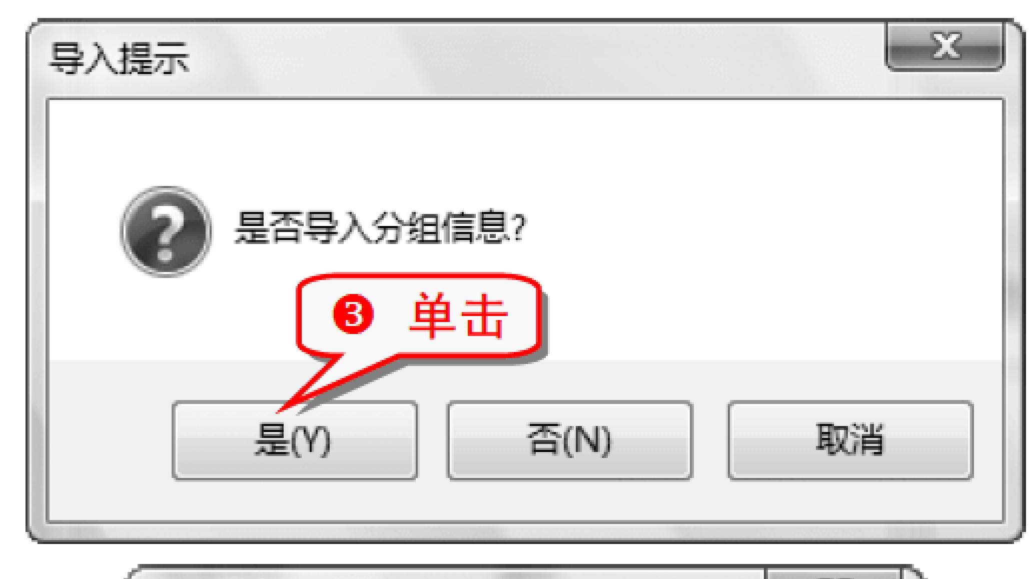


(2) 还原 QQ 表情

将 QQ 表情备份以后就可以随时进行还原。









举一反三

直接双击导出的 QQ 表情文件包，也能对 QQ 表情进行还原。

技巧347　找回 QQ 好友

找回被盗的 QQ 后，往往发现上面的好友全都没有了，不知道怎样找回来。利用以下方法可以恢复丢失的好友。

(1) QQ 好友恢复系统

QQ 好友(群)恢复系统是腾讯公司提供的一项找回 QQ 联系人的服务，向所有 QQ 用户免费开放。

❶ 登录 QQ 好友恢复系统 http://huifu.qq.com/。





注　意　事　项

目前 QQ 好友恢复系统只能恢复最近三个月内被删除的好友。

❺ 成功提交申请信息后，腾讯将在三个工作日内将指定日期内 QQ 上删除的好友恢复。



❻ 此时 QQ 会员只需重新登录 QQ 即可找回被删除的 QQ 列表了，普通用户则还需要进行以下操作。

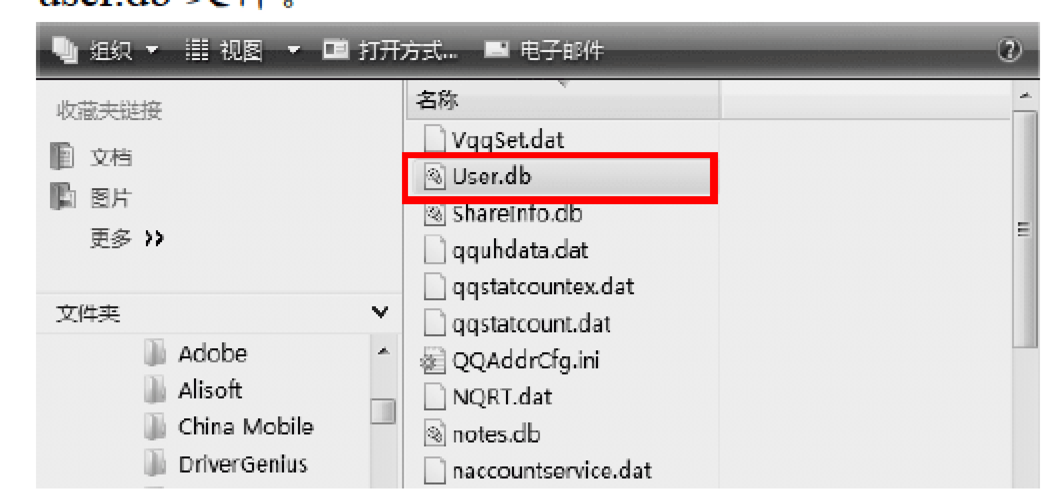


(2) 新 QQ 克隆老 QQ 好友

万一没能找回原来的 QQ，则只能申请一个新的 QQ 号码，下面介绍如何将原来 QQ 上的好友克隆到新的 QQ 上。

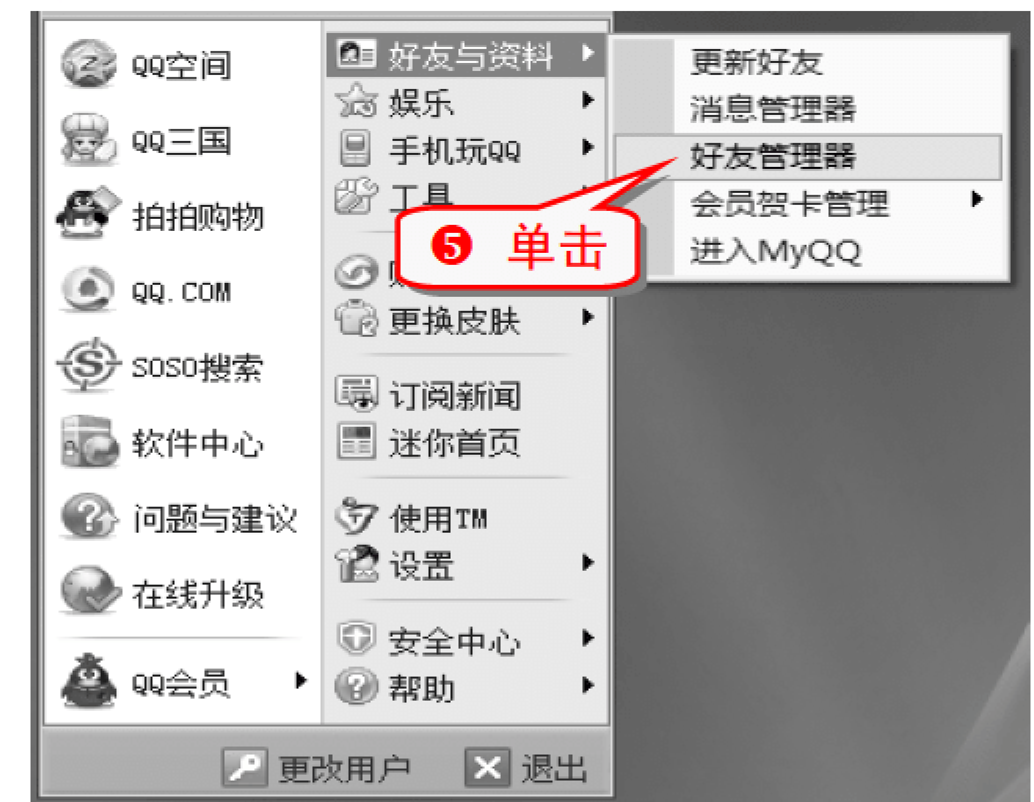
❶ 使用新申请的 QQ 登录一次，然后关闭 QQ，建立新 QQ 的相关文件。

❷ 打开 QQ 的安装目录，找到原 QQ 号码文件夹下的 user.db 文件。



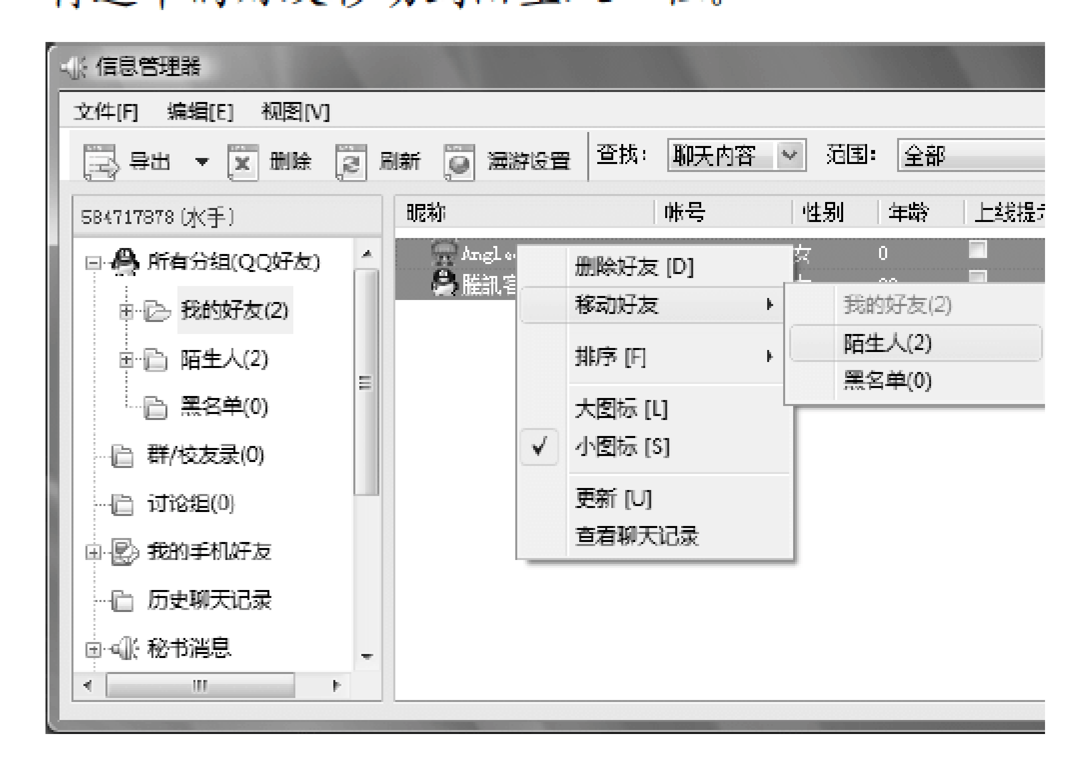
❸ 复制 user.db 文件至新 QQ 号码的目录下，替换掉新 QQ 号码下的该文件。

❹ 登录新的 QQ，出现原来 QQ 的好友列表，不过头像都是灰色的。

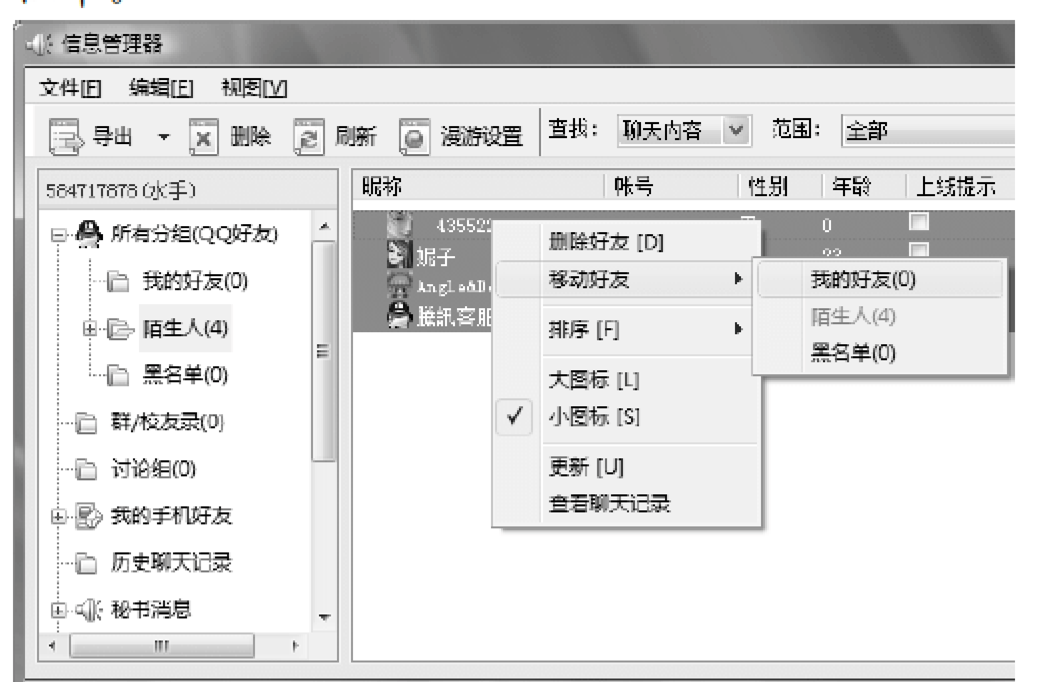




❻ 在好友列表里选中想要加的人，可以拖选多个好友，将选中的好友移动到陌生人一栏。



❼ 在陌生人列表中选中这些好友将其移动到我的好友栏中。



❽ 确认好友添加对话框即可完成好友的克隆。

技巧348　批量导出/导入 MSN 联系人

由于工作等原因用户可能需要更换 MSN，逐个添加联系人，工作量非常大，利用 MSN 的“联系人”功能可以非常方便地实现联系人搬家。

(1) 批量导出联系人

❶ 登录 MSN，进行如下操作。





(2) 批量导入联系人

❶ 登录需要导入联系人的 MSN，选择“联系人”→“导入即时消息联系人”命令，弹出“导入即时消息联系人列表”对话框。



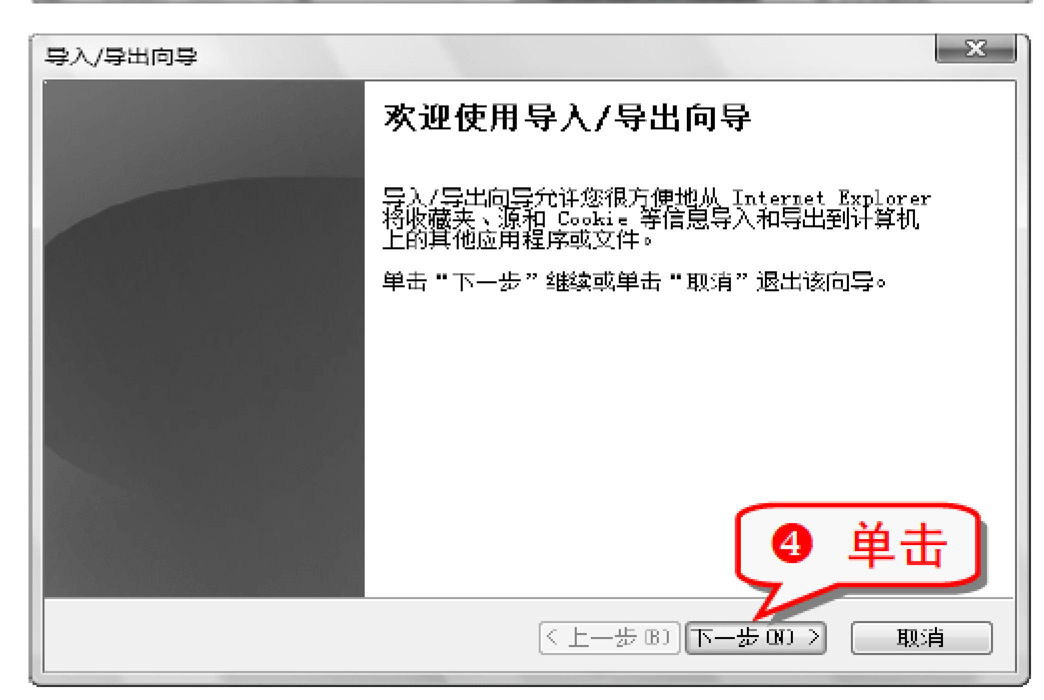
技巧349　快速导出/导入收藏夹

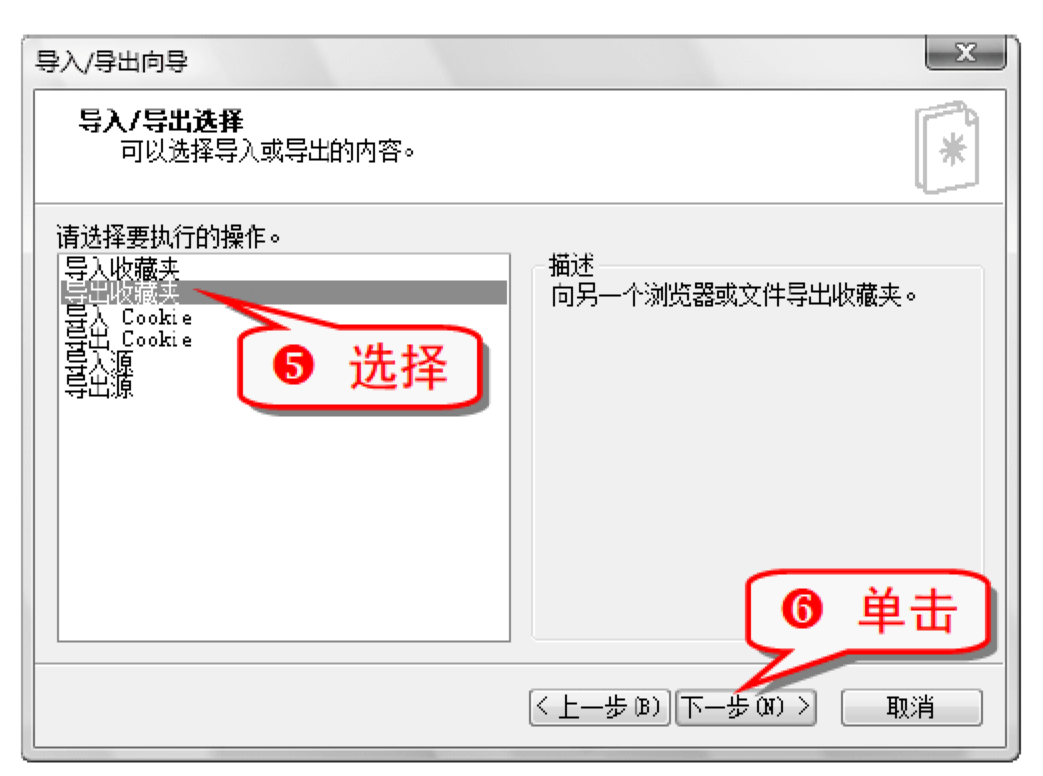
导出收藏夹可以在系统崩溃后恢复收藏夹，按照“导入/导出向导”便可轻松实现收藏夹的导入导出。

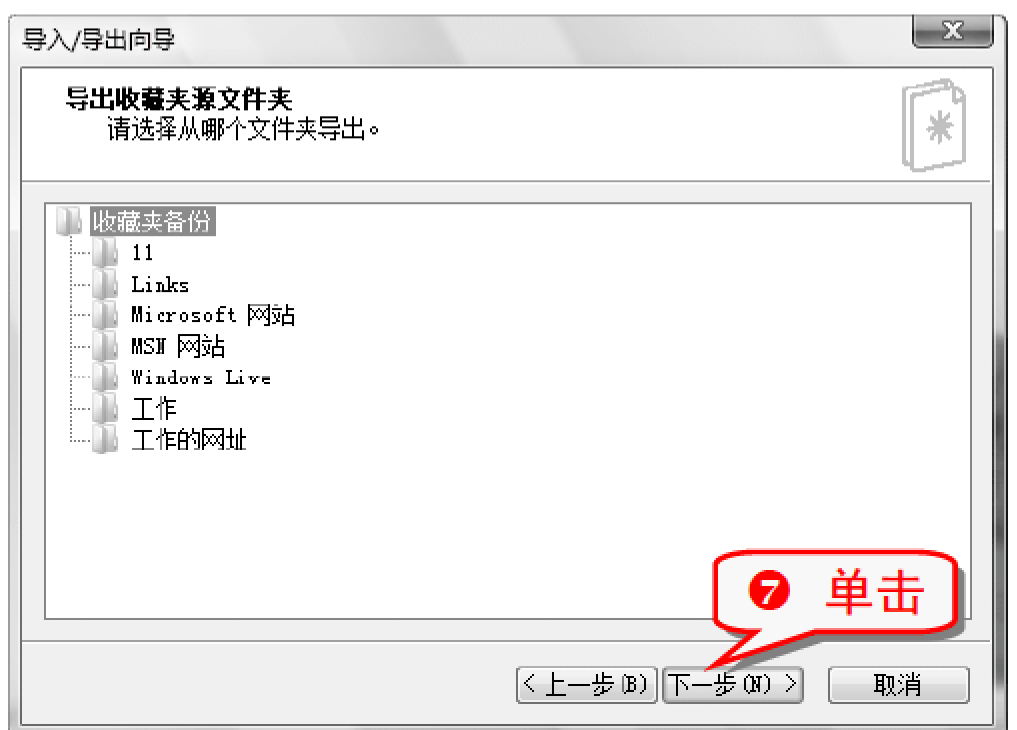
(1) 导出收藏夹

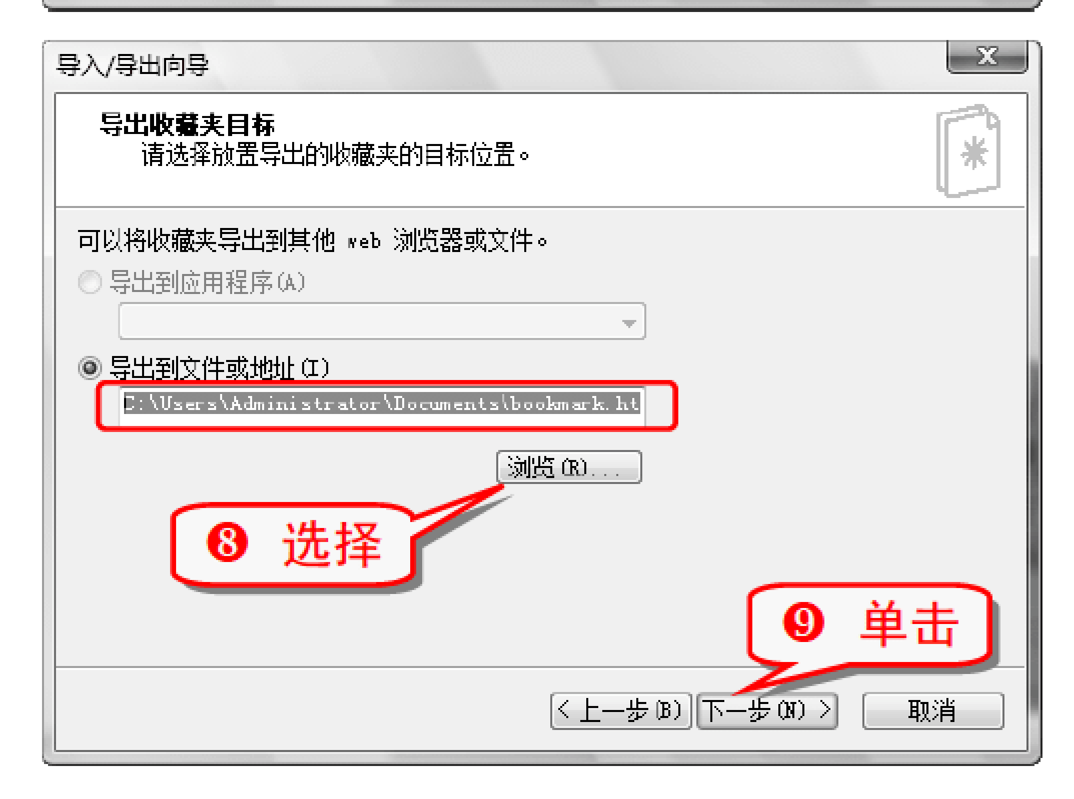
❶ 打开 IE 浏览器。



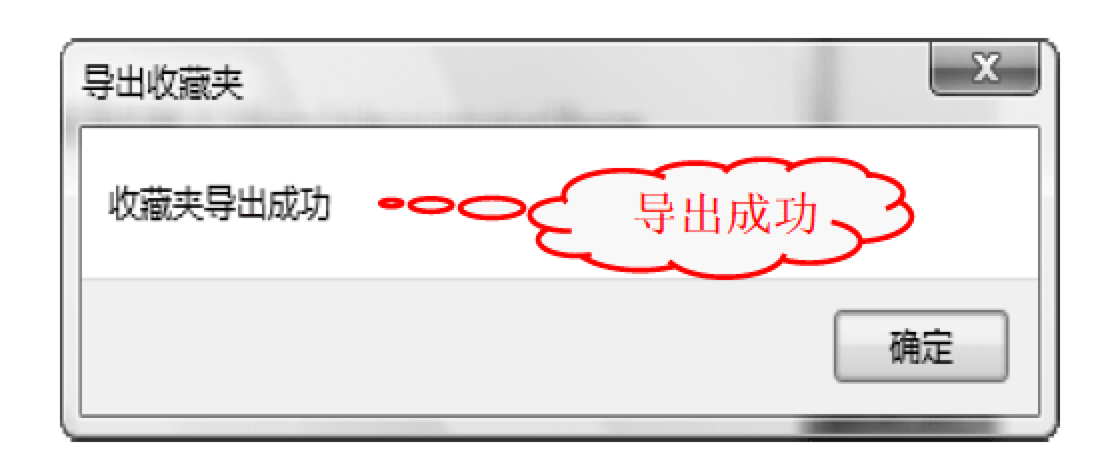












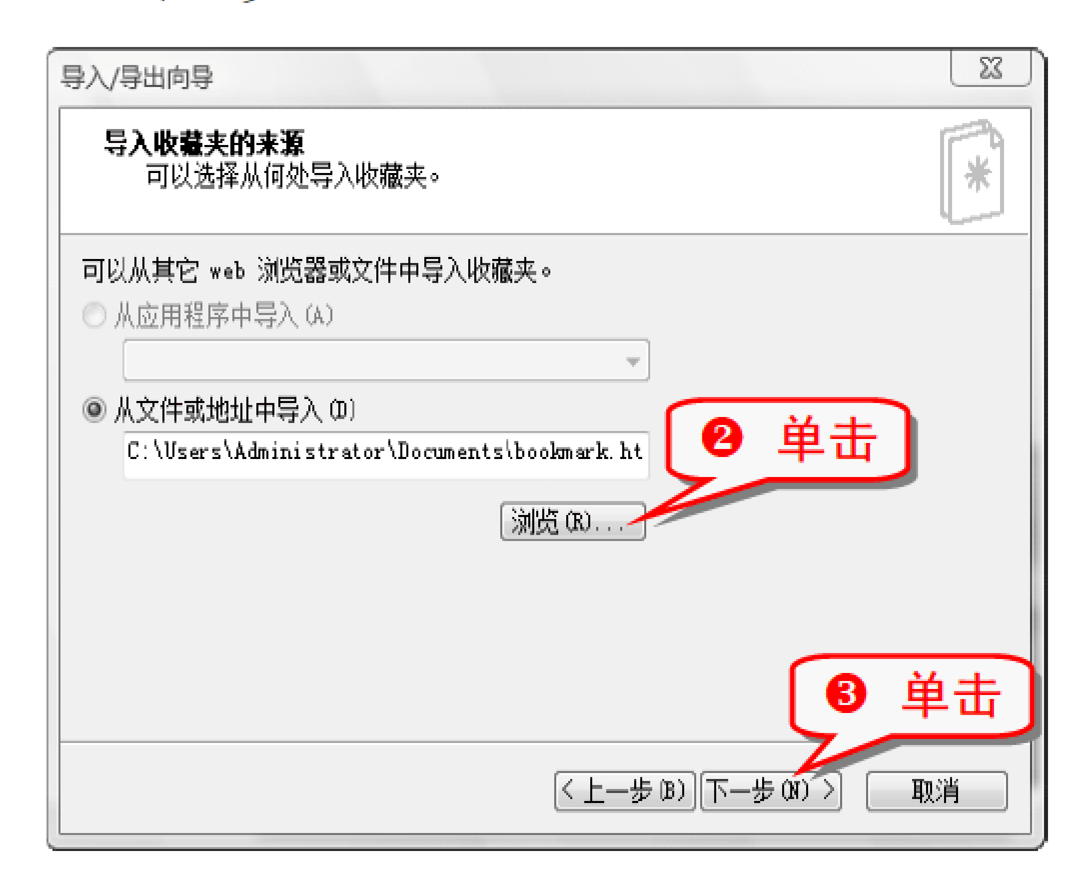
注 意 事 项

在第❽步操作时，默认的路径是保存在 C 盘的 Documents 文件夹中，创建一个名为 Bookmark.htm 的文件，单击“浏览”按钮指定新的保存路径和文件名。

(2) 导入收藏夹

导入和导出的操作步骤相似，只要按照“导入/导出向导”提示就可以轻松实现导入工作。

❶ 在打开的 IE 浏览器中，单击按钮，选择“导入和导出”命令，在弹出的“导入/导出向导”对话框中单击“下一步”按钮。







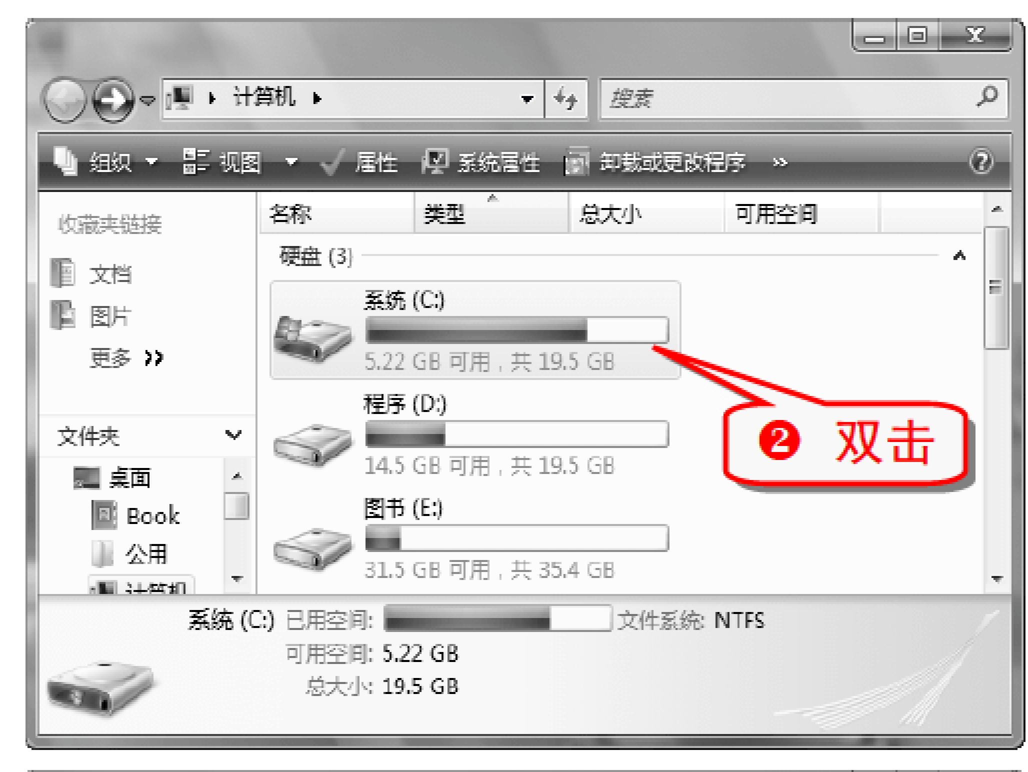


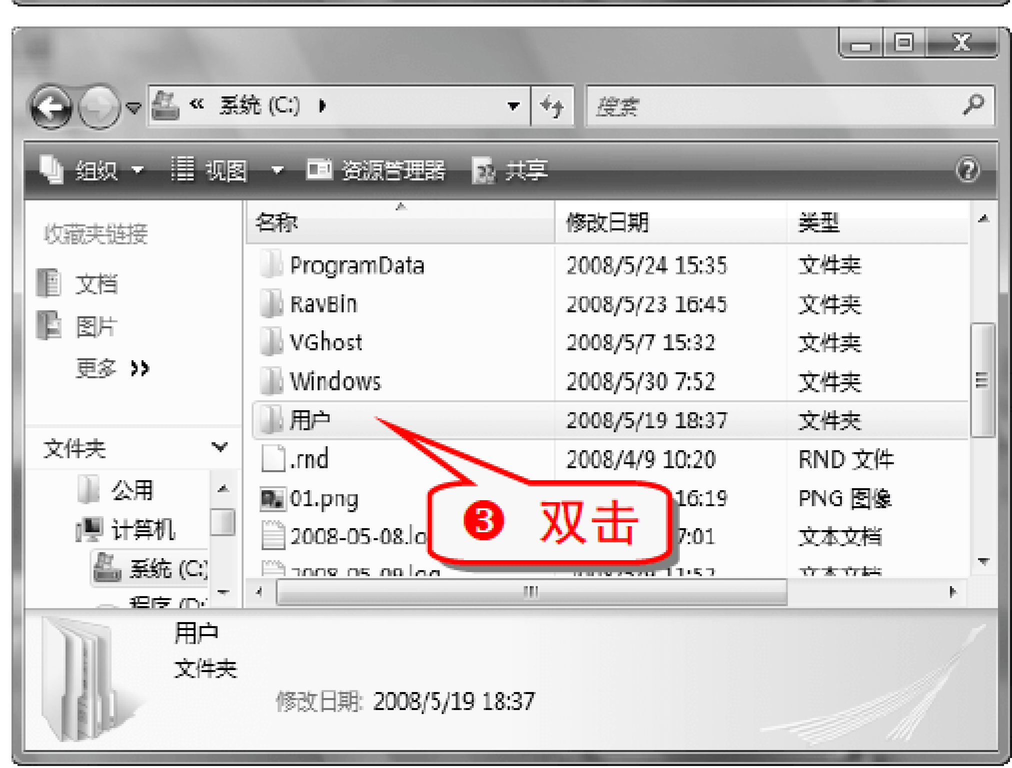


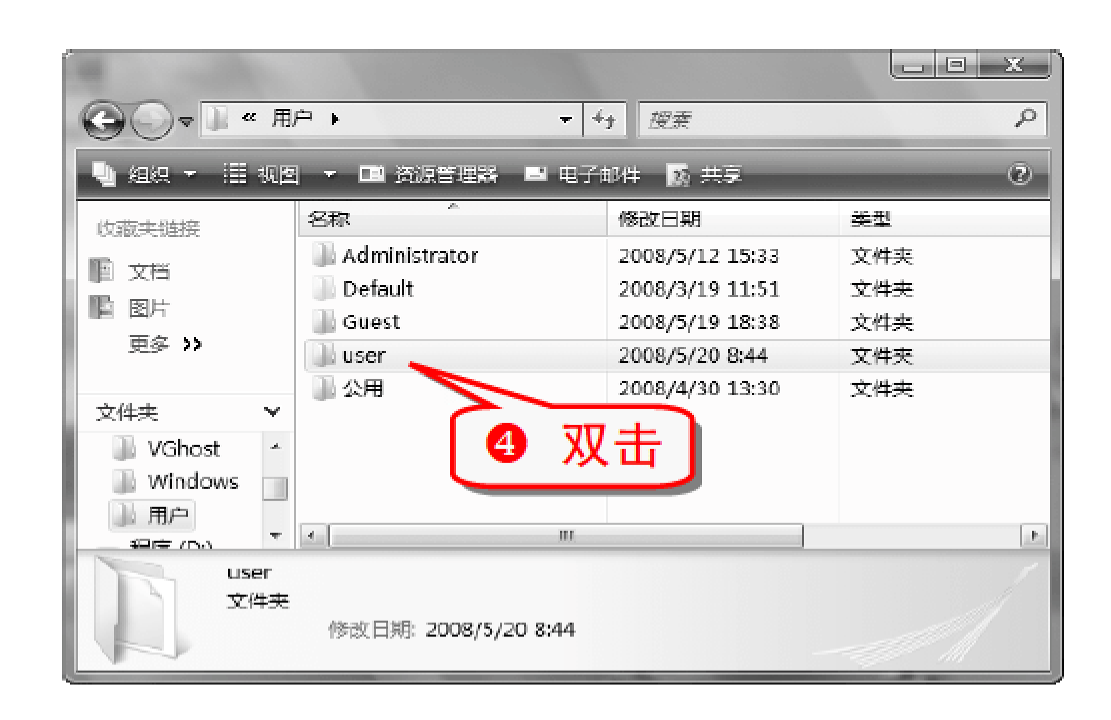
技巧350　手动备份收藏夹

通过找到 IE 收藏夹在 C 盘中的位置，将里面的网页复制一份，放在别的磁盘文件中，下次 IE 重装或系统重装后，直接将其复制进去就可以。

❶ 双击“计算机”图标，打开“计算机”窗口。







注　意　事　项

一个电脑通常有多个账户，每个账户都有自己的 IE 收藏夹，这里要备份账户名为 user 的 IE 收藏夹。

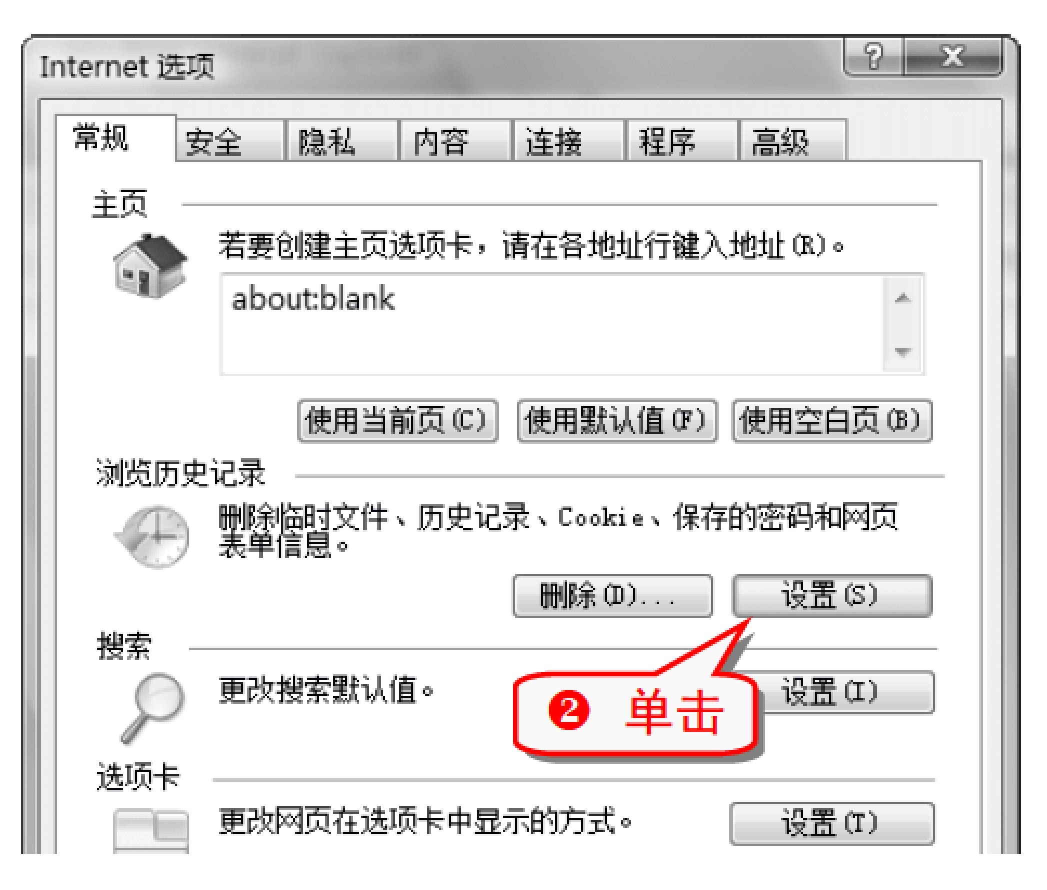


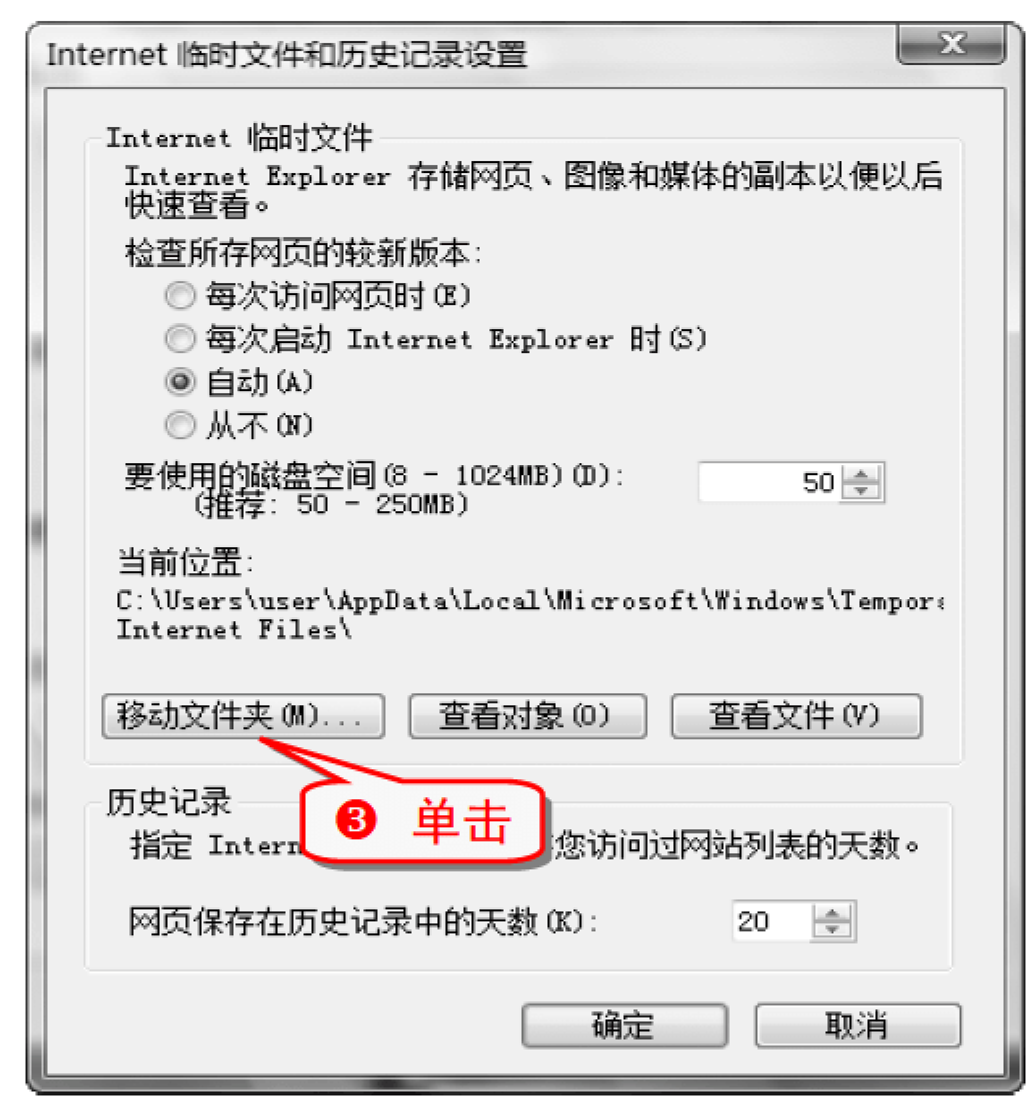
❼ 在非系统盘中新建一个文件夹，将收藏夹复制进去。

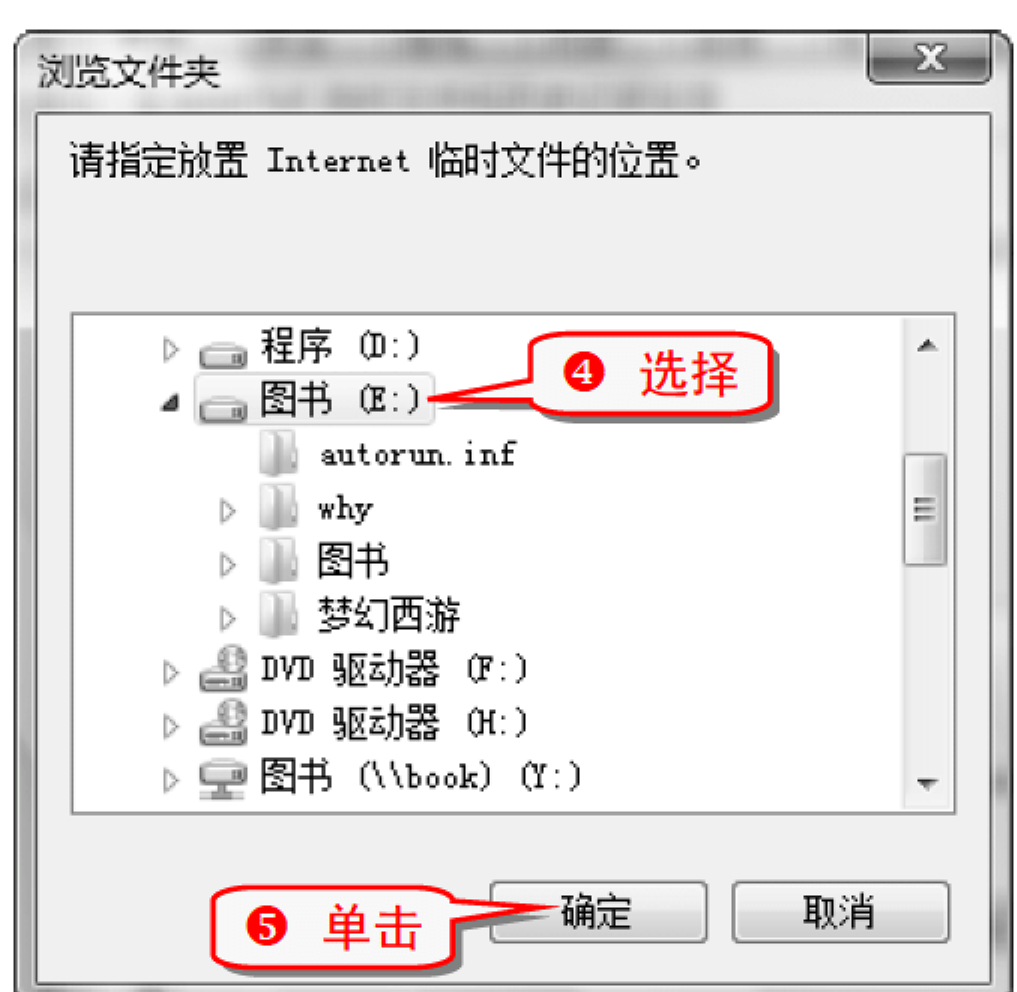
技巧351　IE 缓存的备份

每次打开一个网页，IE 会自动创建一份该网页文字和图像的缓存文件。当再次打开该页，IE 会检查网站服务器上该页的变化。IE 会在缓存中保留网页到硬盘这样设计的目的是为了更快地装载页面。

❶ 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，打开“Internet 选项”对话框。







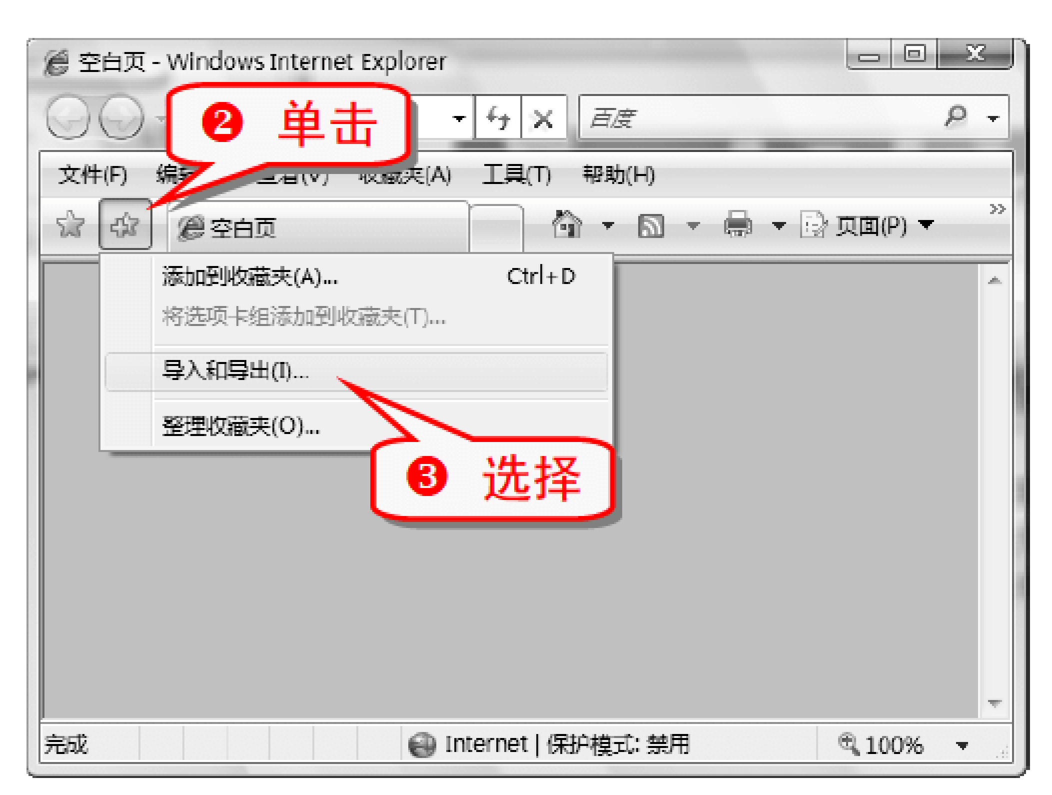
> **注 意 事 项**
>
> 选择一个不是在系统盘下的目录作为IE临时文件夹的存储路径。

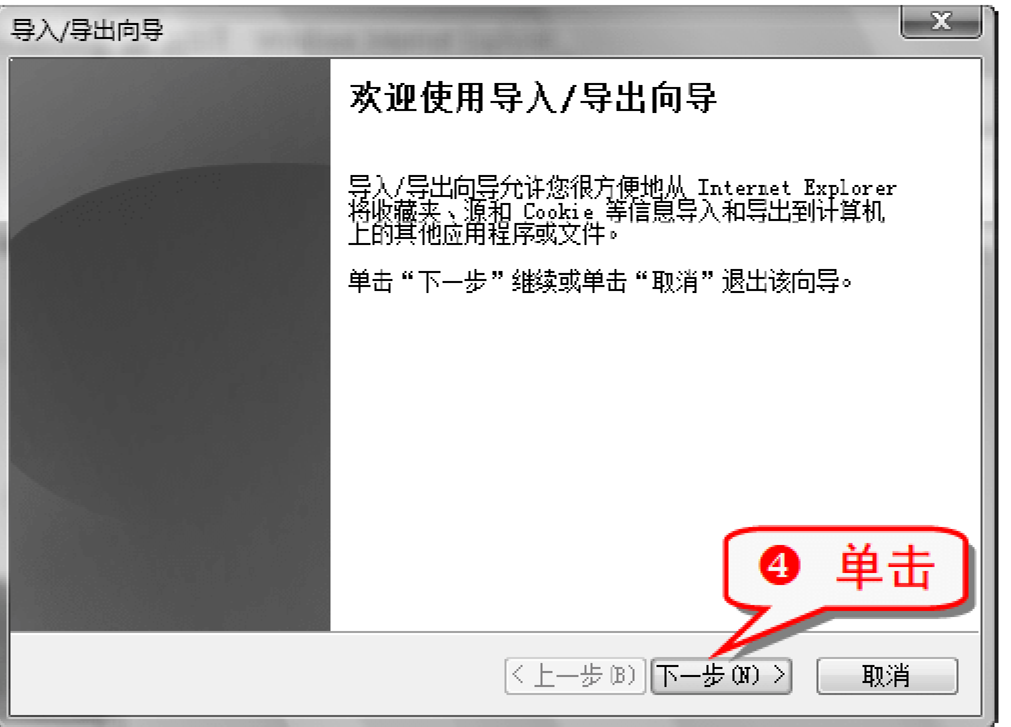
技巧352 Cookie 的备份与还原

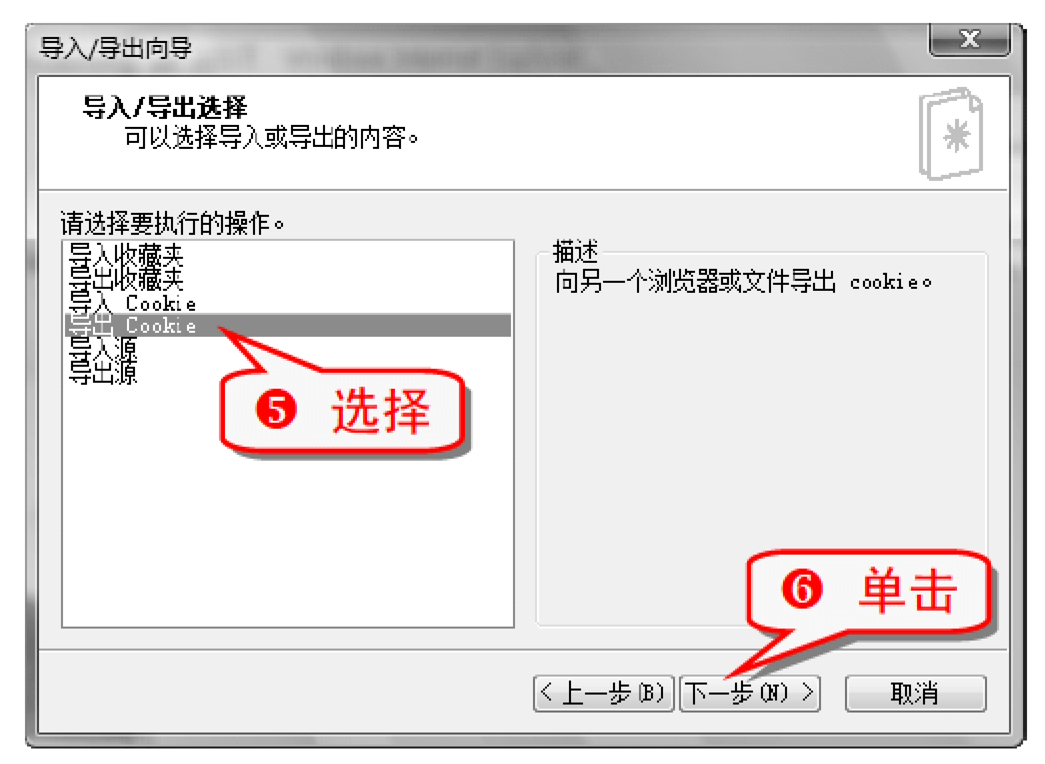
如果没有 Cookie，每次登录时都需要输入账户和密码，而有了这个“小甜饼”，就能避免这种麻烦。为了避免今后“重陷泥沼”，应该保存这些有用的 Cookie。

(1) 将 Cookie 文件导出

❶ 打开 IE 浏览器。

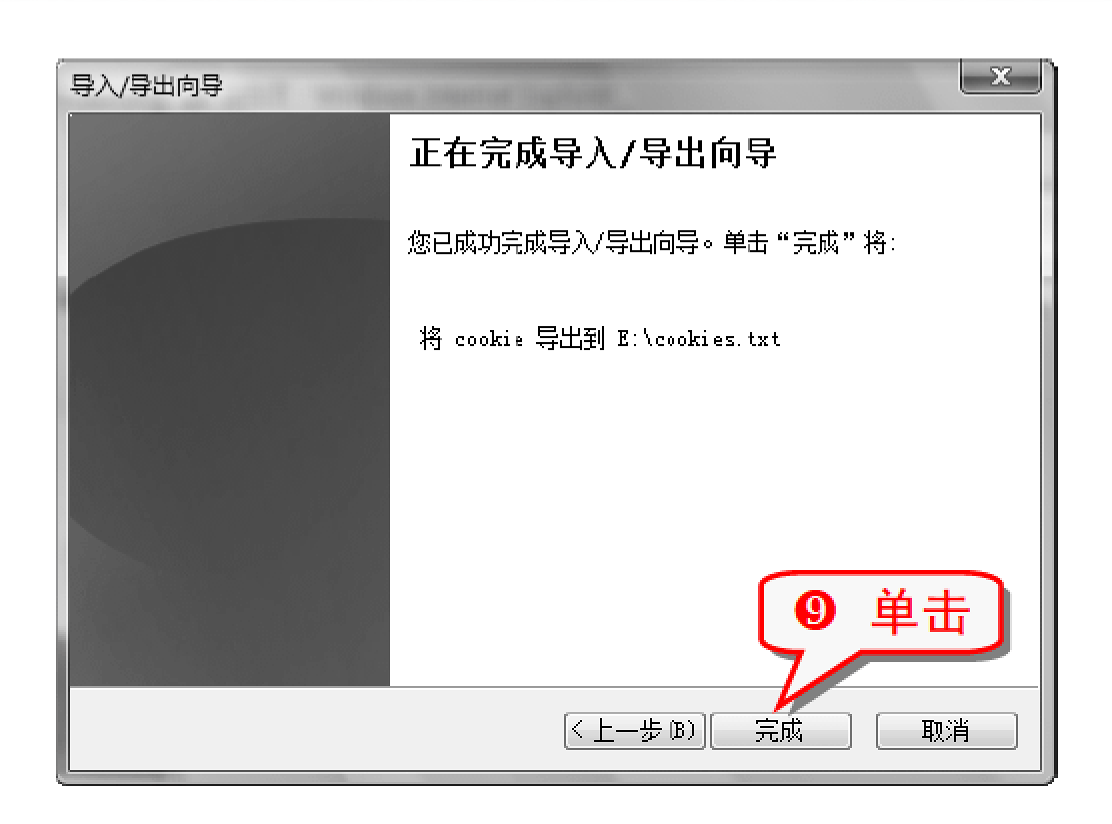






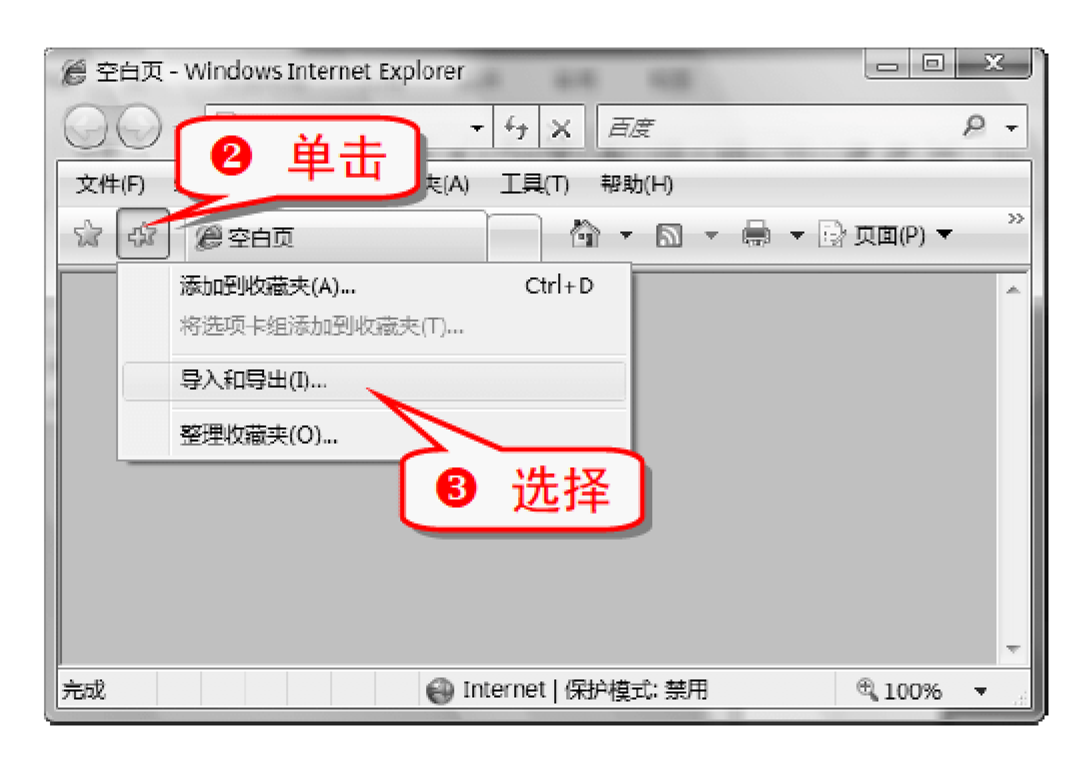


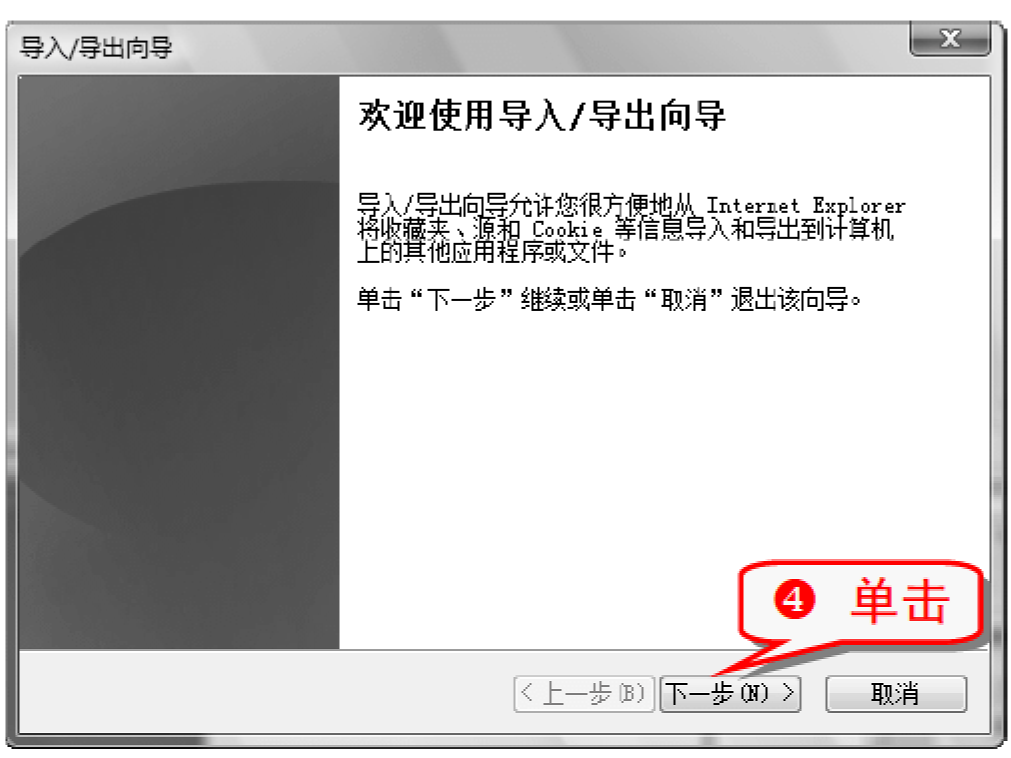


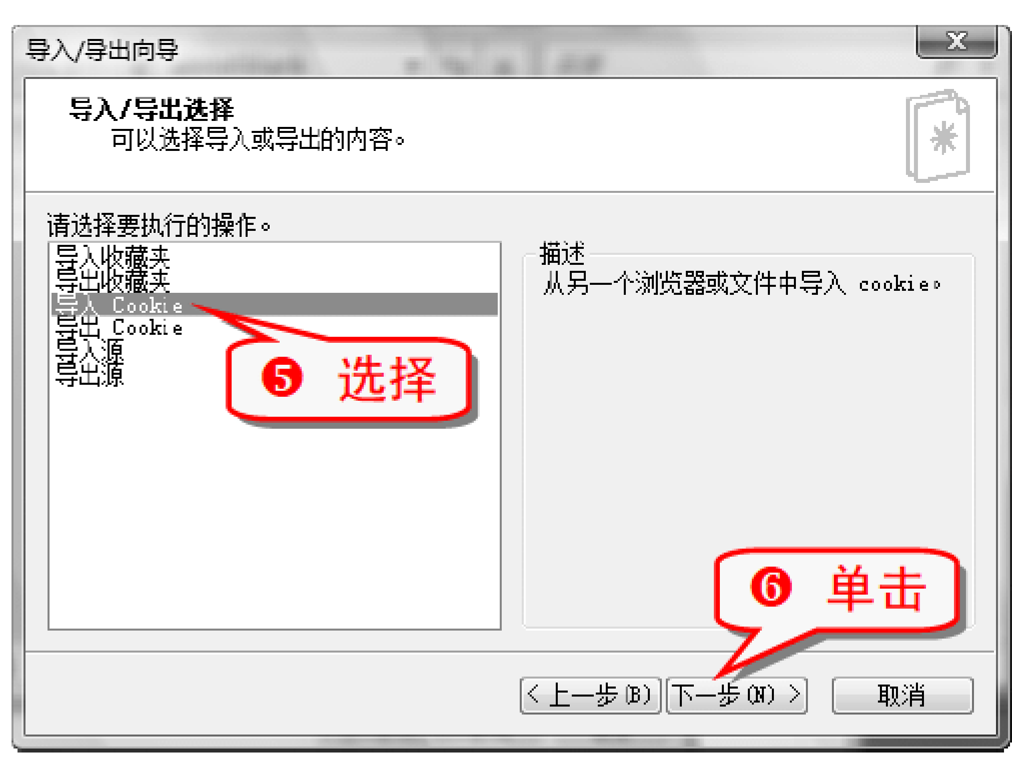


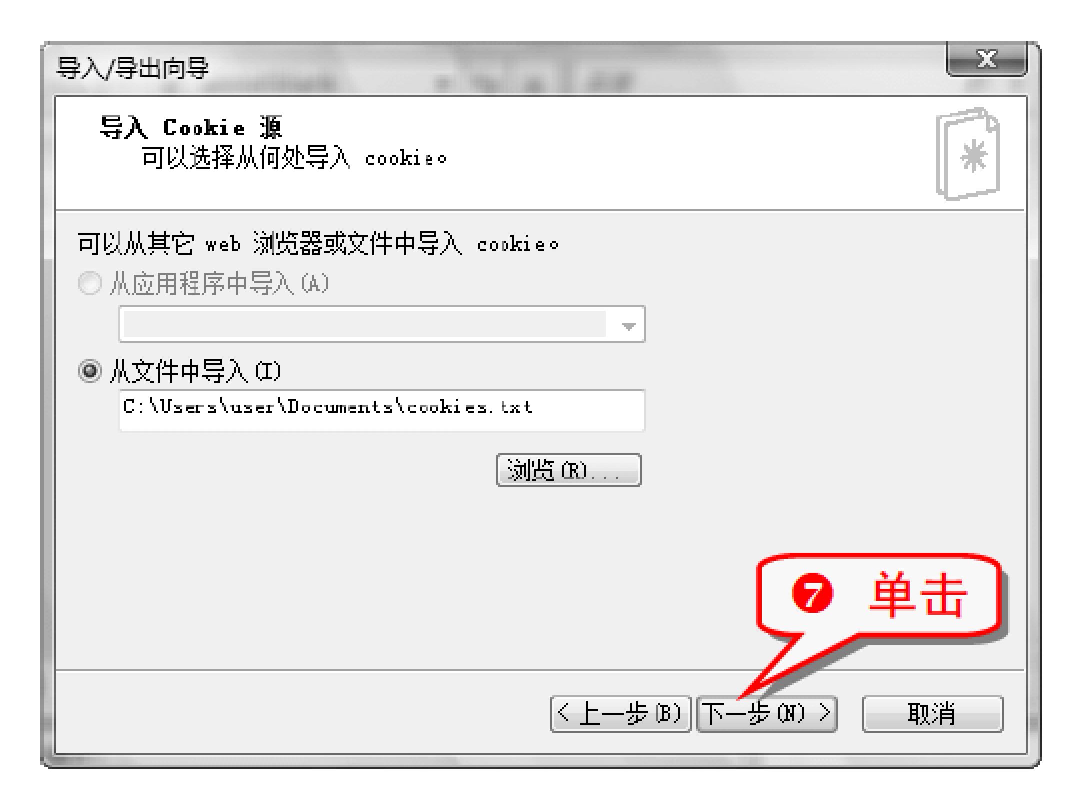
(2) 将 Cookie 文件导入

❶ 打开 IE 浏览器。

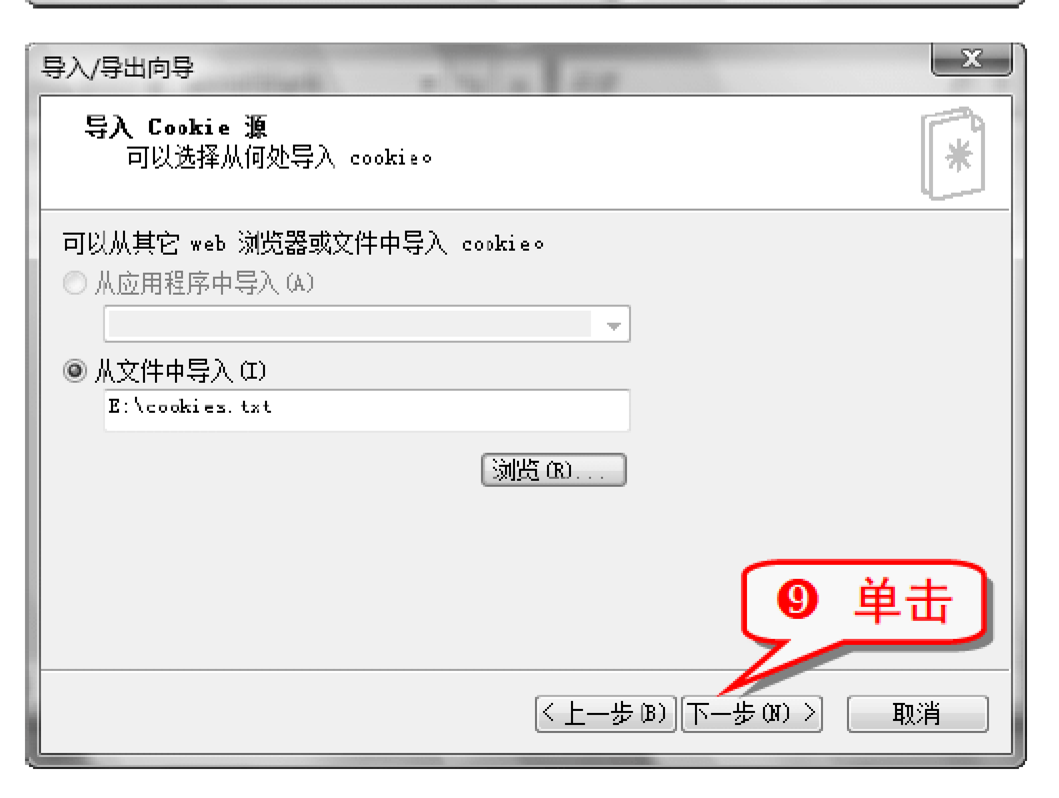


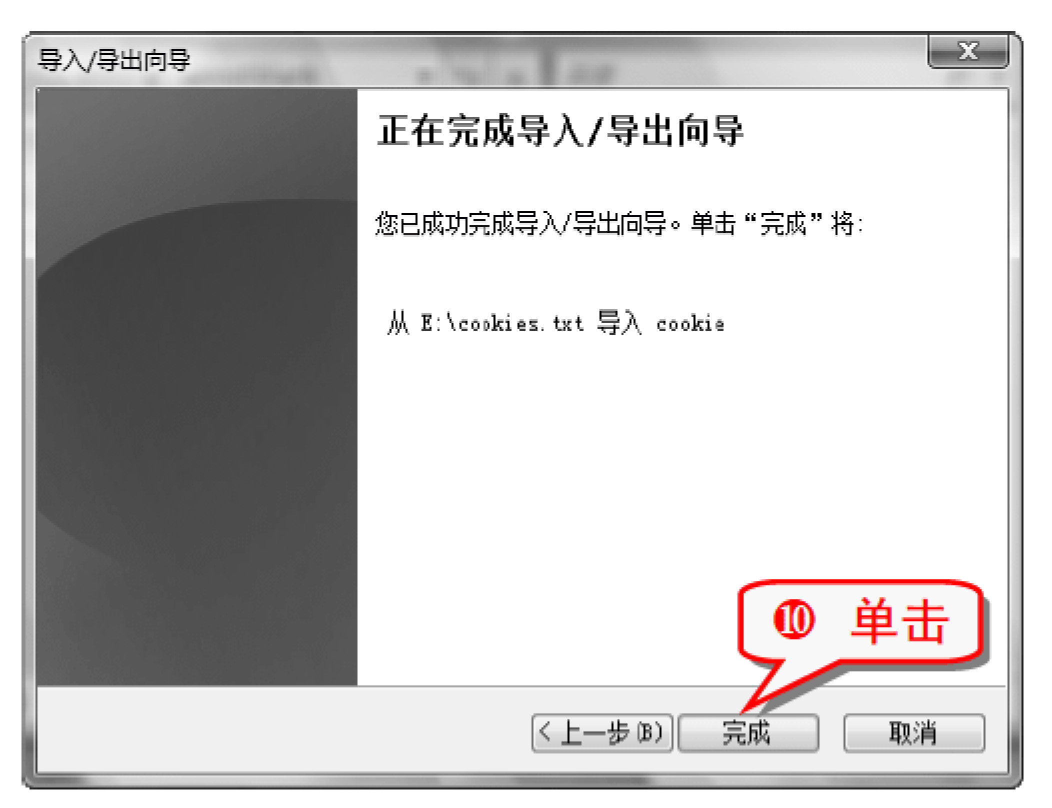








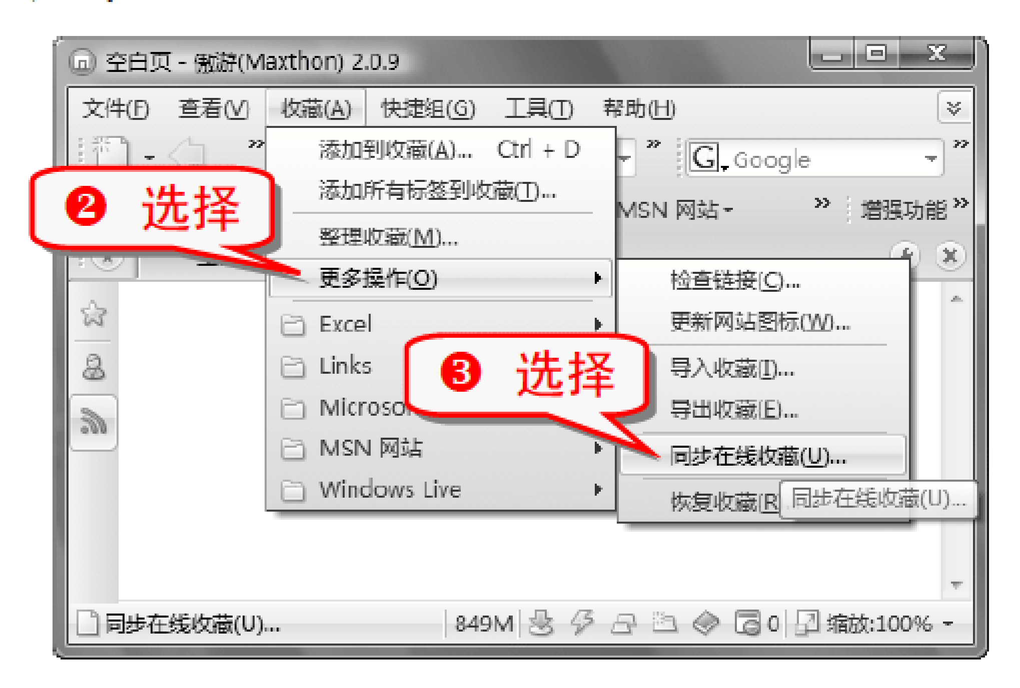




技巧353 在线备份与恢复收藏夹

傲游(Maxthon)2.0 的收藏夹服务可以实现本地收藏夹和网络收藏夹之间的同步。

❶ 启动傲游浏览器，打开“收藏”菜单，进行同步在线收藏。



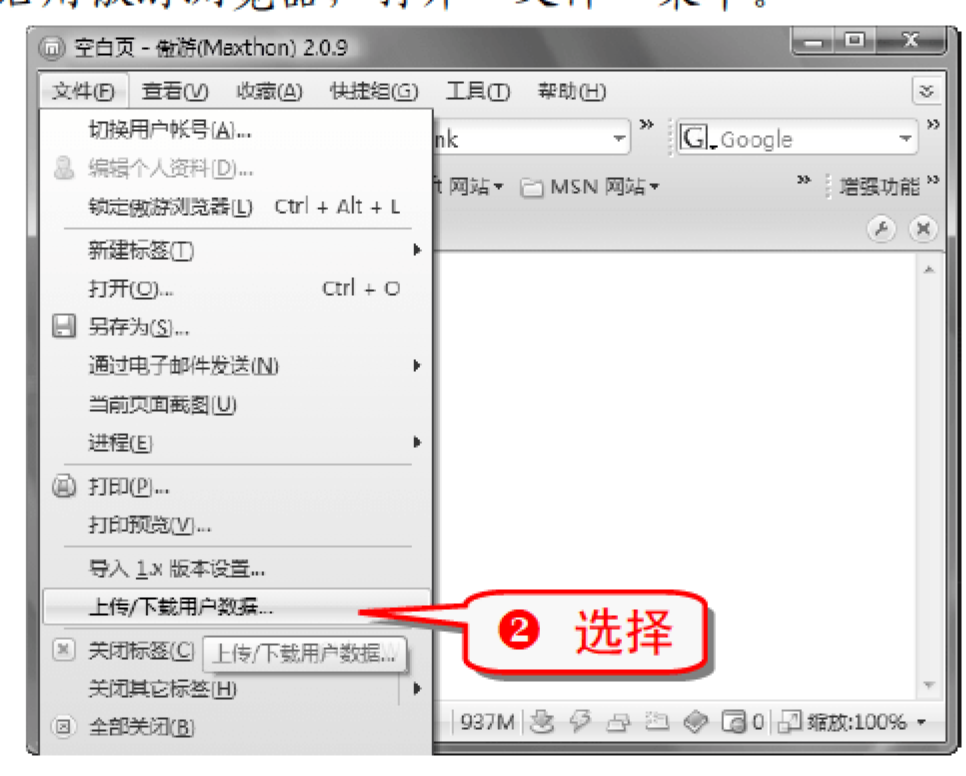
❹ 傲游的服务器上会保留不同时间的多个收藏夹备份，如果出现收藏夹丢失等状况，可以访问 http://favrecover.maxthon.com/ 将收藏夹恢复到其历史版本。

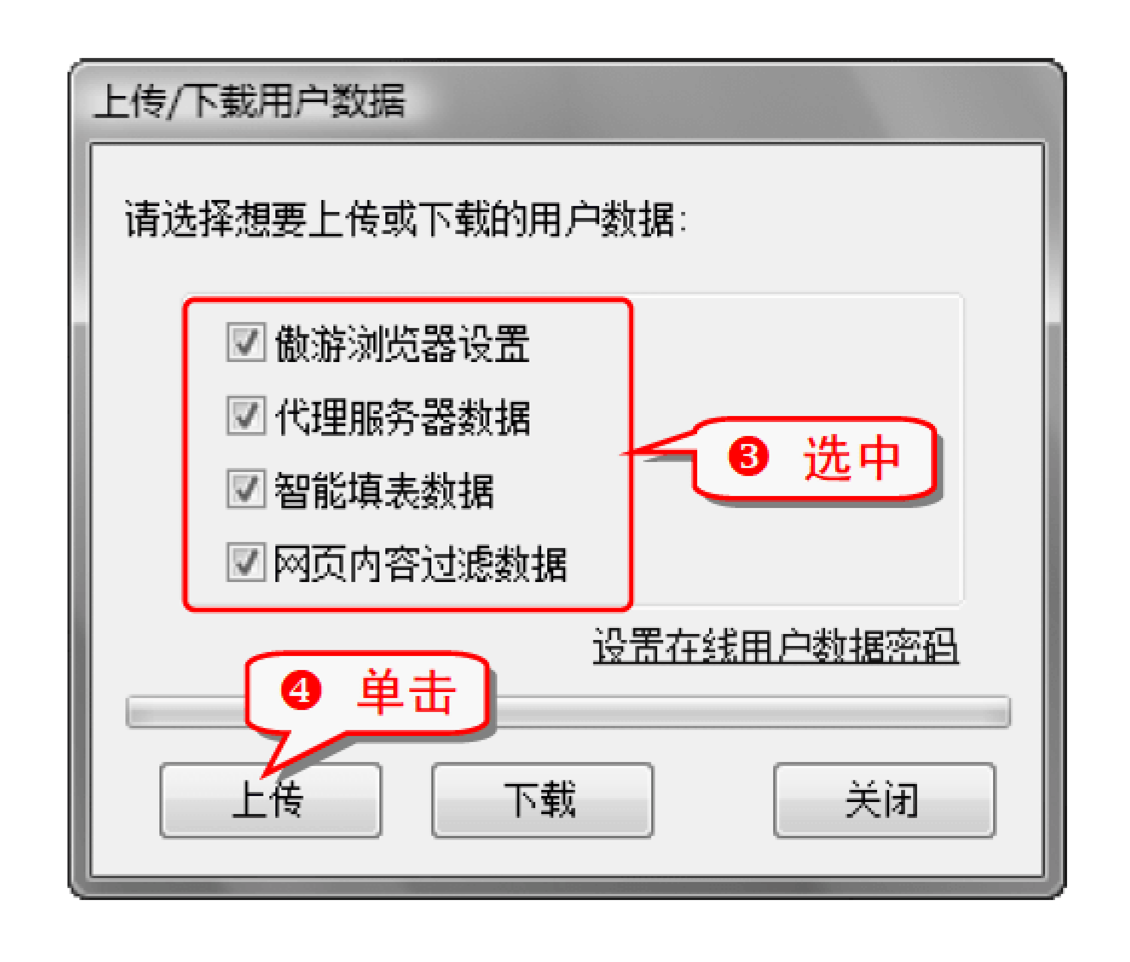


技巧354 备份浏览器设置

每次重新安装浏览器，都需要对浏览器进行再次设置，非常麻烦，最新版的 Maxthon 2.0 支持把用户设置备份到服务器，重新安装的时候只要下载原设置就可以了。

❶ 启用傲游浏览器，打开“文件”菜单。





技巧355 备份网络设置参数

局域网内的电脑需要设置相关的网络参数，以保证局域网内用户可互相访问、连接互联网以及整个局域网的稳定。将这些网络设置参数备份下来，当电脑重装系统后就可以快速正确地重新设置网络参数。

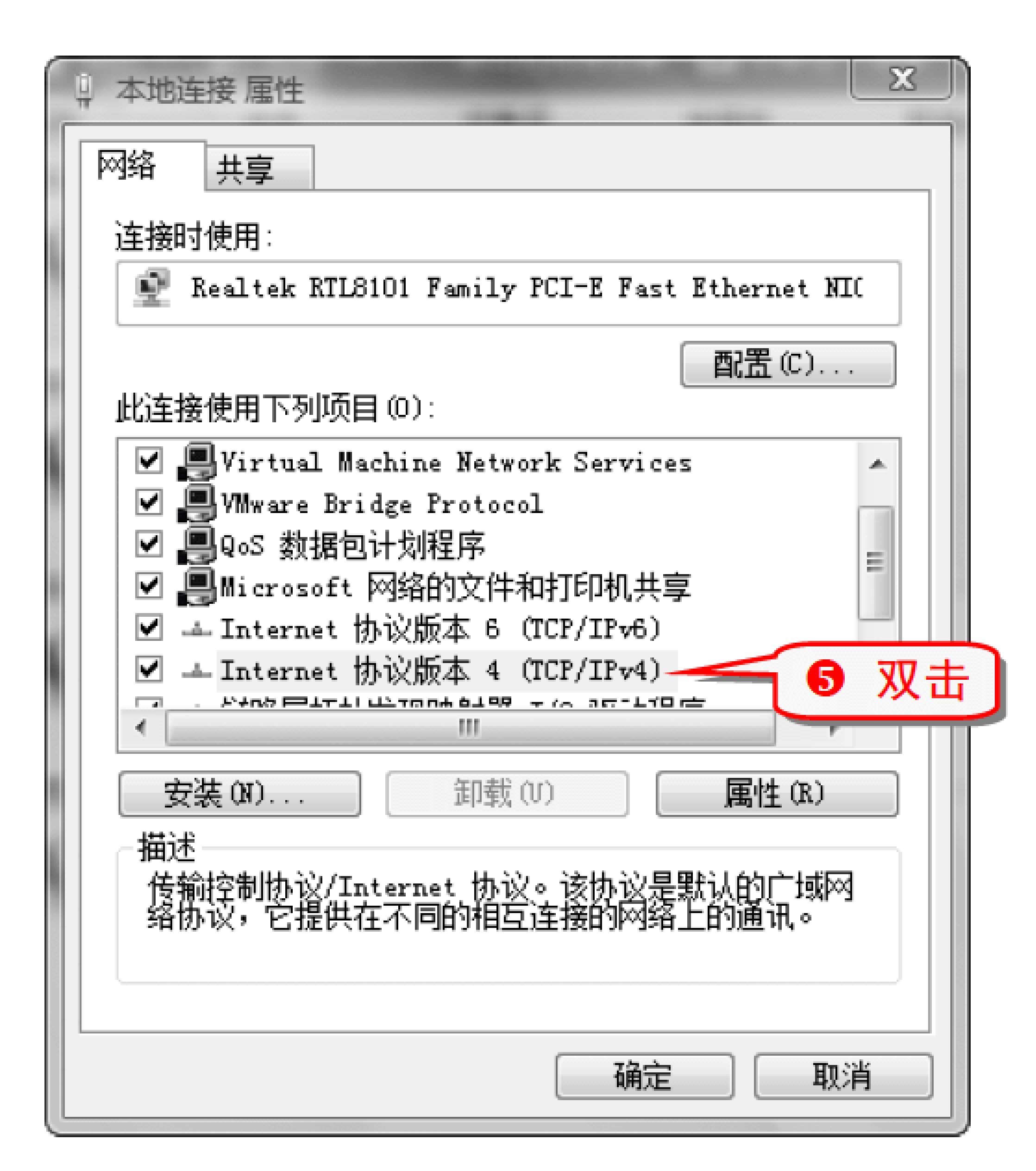
❶ 右击桌面上的“网络”图标，在弹出的对话框中选择“属性”选项。

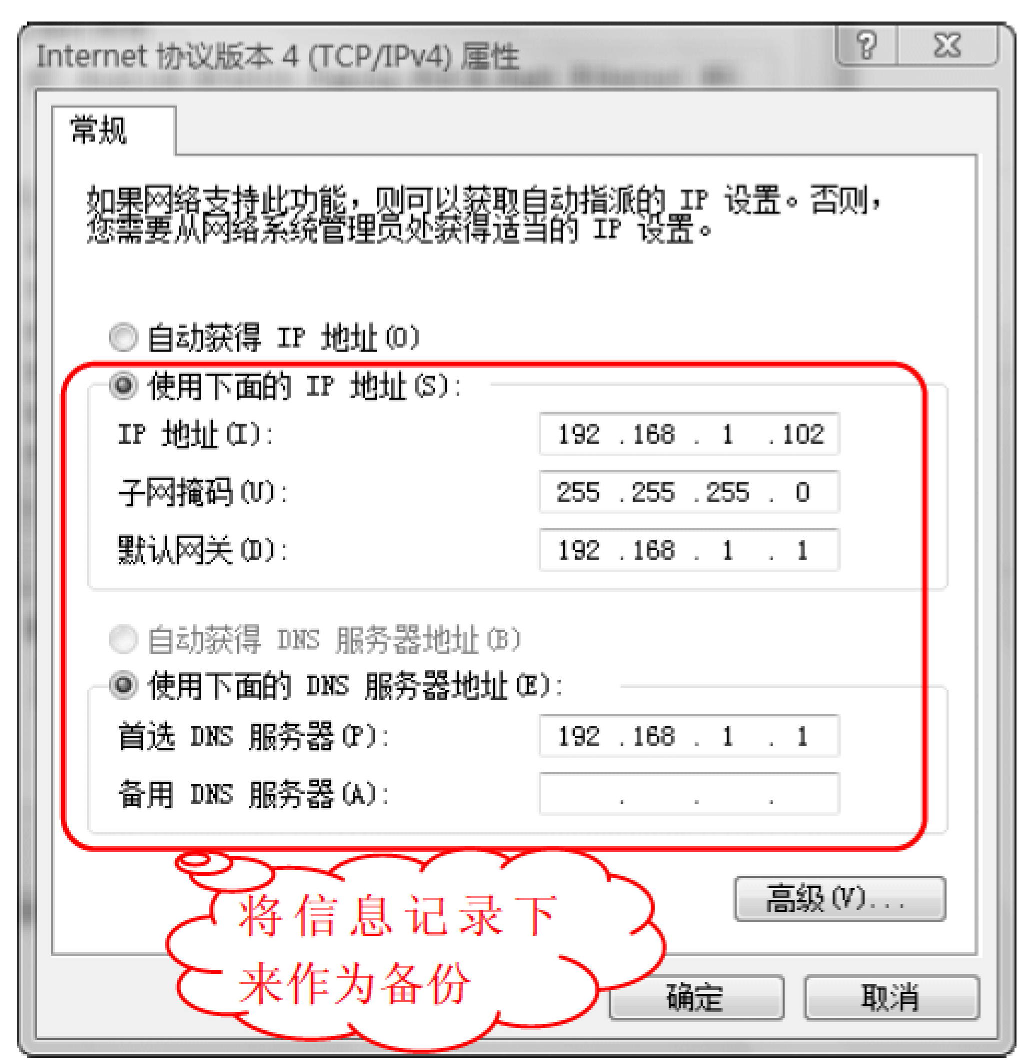


❸ 右击“本地连接”选项。









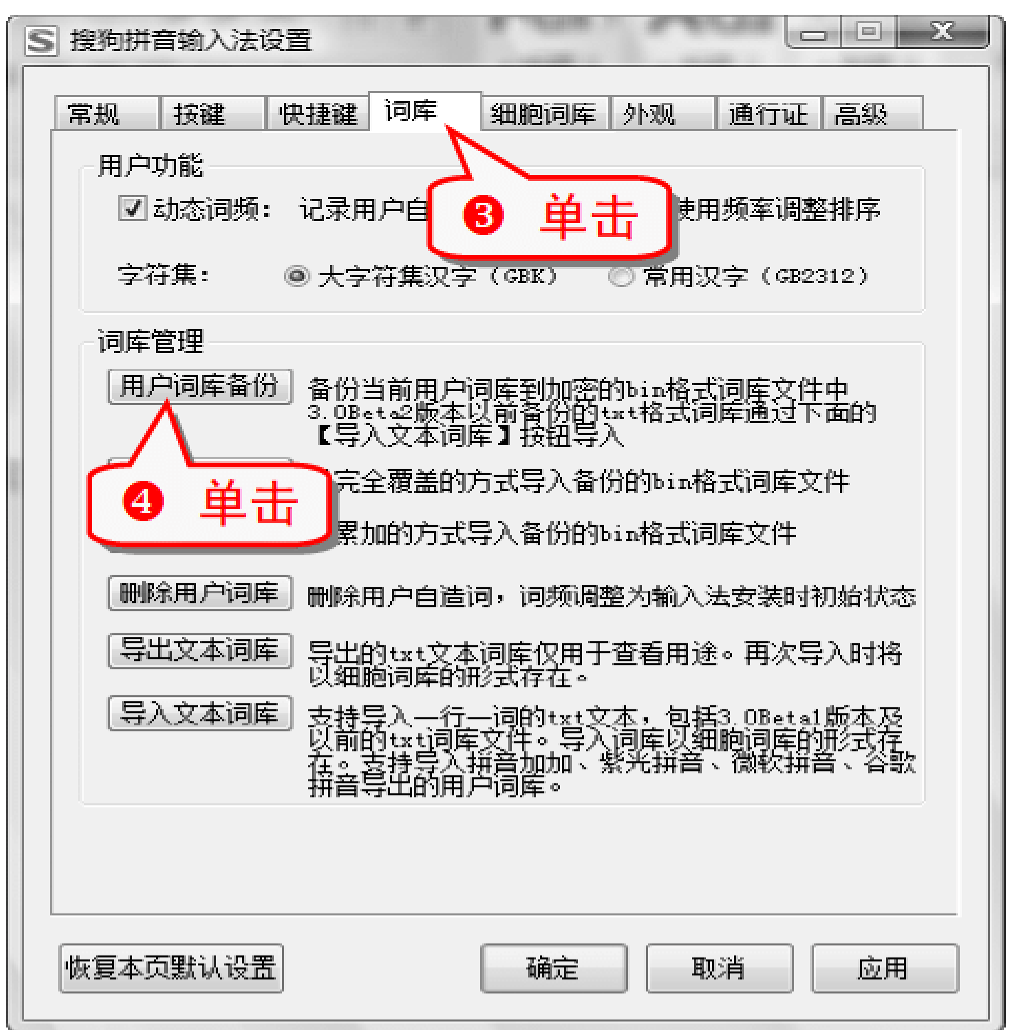
技巧356　搜狗输入法的备份与恢复

搜狗输入法是现在比较流行的输入法之一，会自动记忆用户的输入习惯，当搜狗输入法重装时，这些输入习惯就会消失。将其用户词库备份以后就不用担心这个问题了。

(1) 备份用户词库

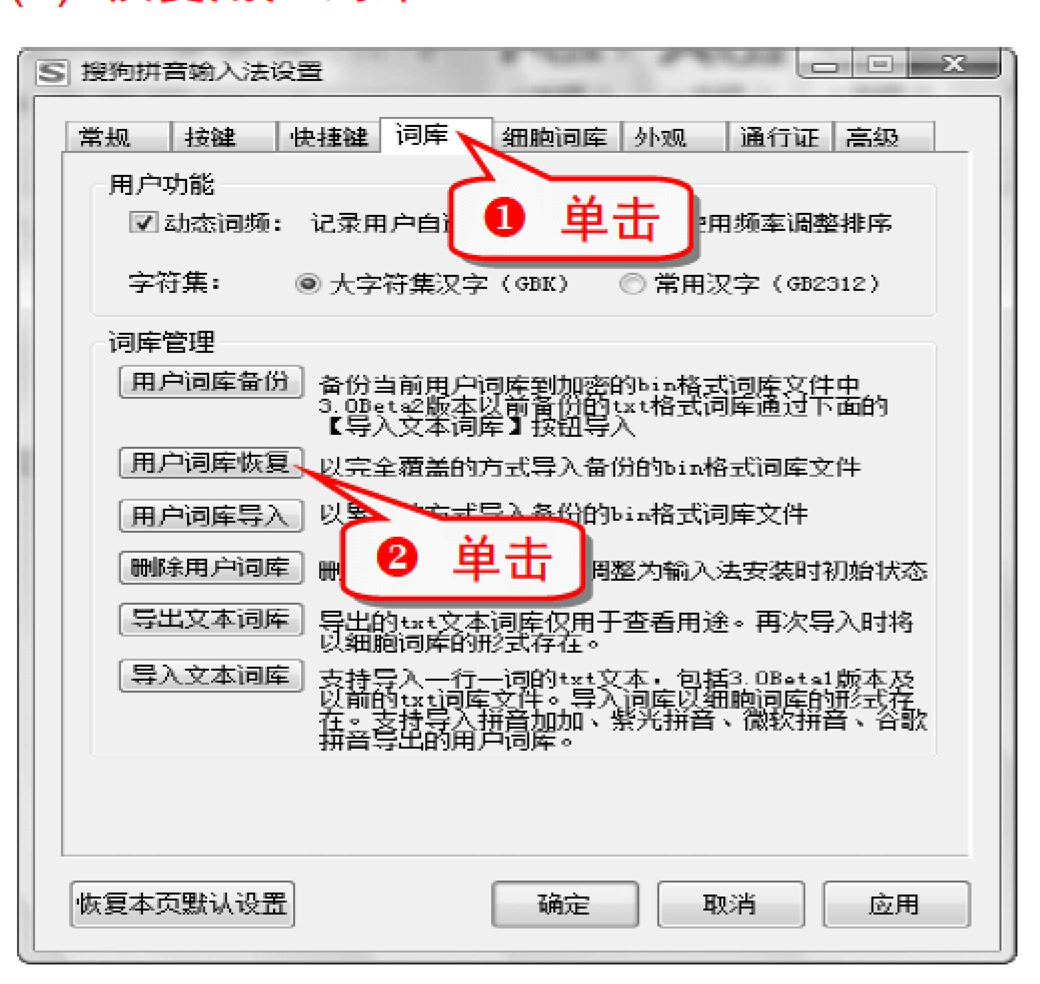


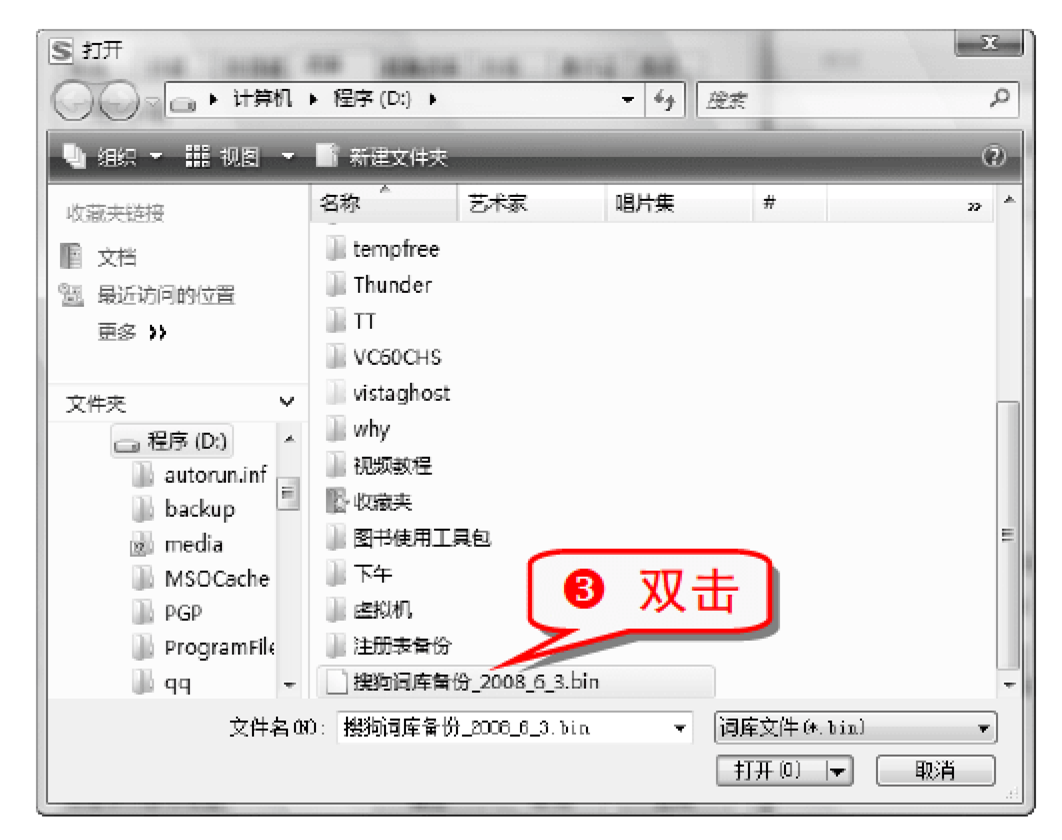


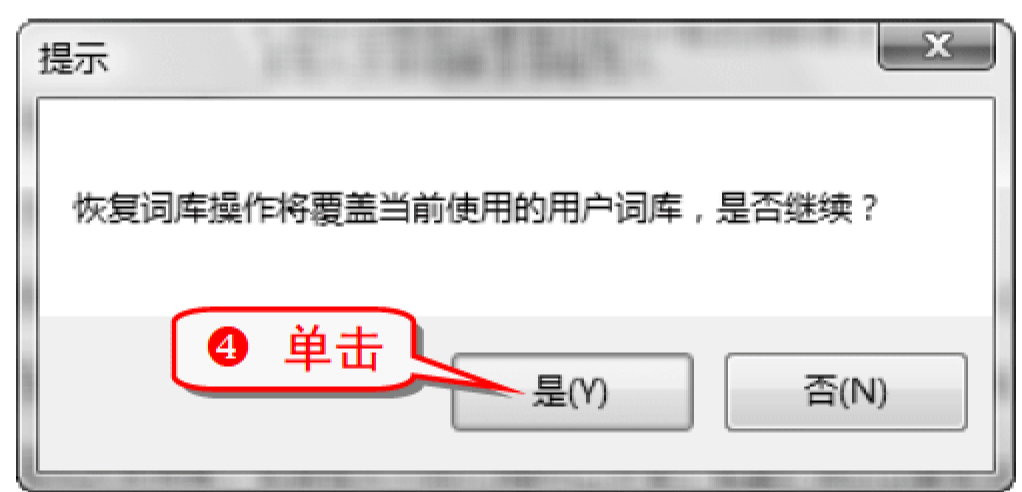




(2) 恢复用户词库







技巧357　备份 WinRAR 的设置

对 WinRAR 进行个性化设置，使 WinRAR 工作起来更符合自己的习惯，从而提高效率。有两种方法可以备份 WinRAR 的设置。

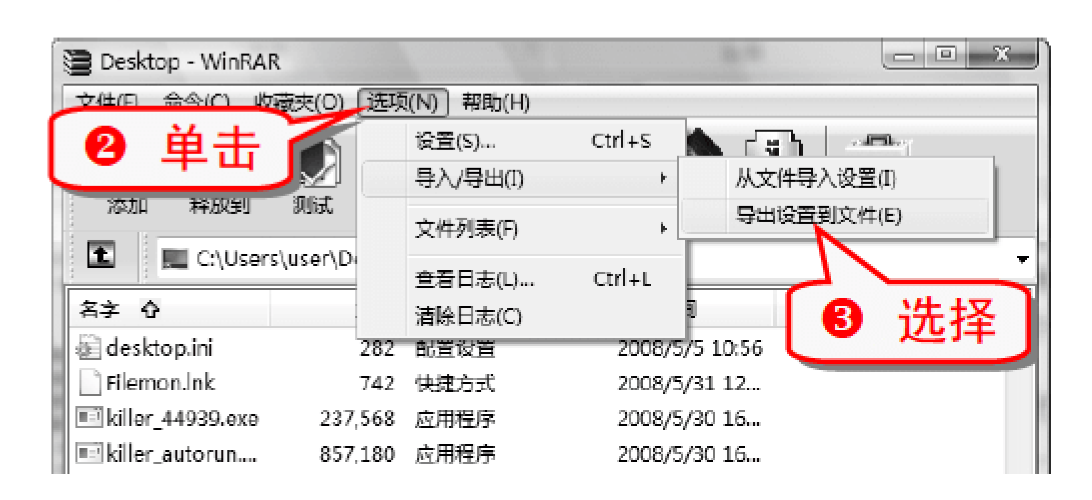
(1) 直接备份注册表

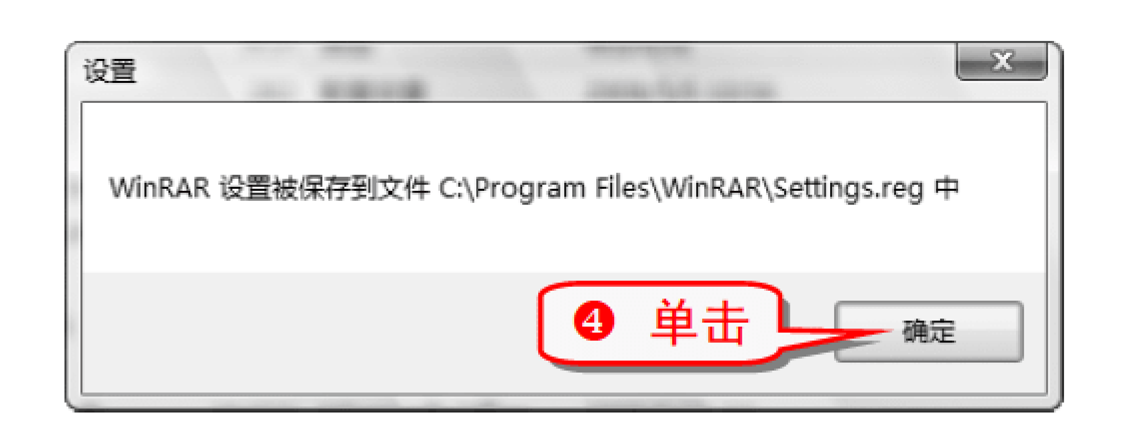
打开注册表编辑器，定位到 HKEY_CURRENT_USER\Software\WinRAR 分支，其下保存了设置对话框所对应的所有配置内容，比如 HKEY_CURRENT_USER\Software\WinRAR\Compression 下的 DefFolder 子键，定义的是压缩文件的默认保存位置，而 HKEY_CURRENT_USER\Software\WinRAR\Extraction 下的 DefFolder 子键，定义的是默认释放位置。可以直接导出该分支，假设保存为"WinRAR 设置.reg"，以后恢复的时候，只需双击该文件即可。

(2) 利用 WinRAR 自带的导入导出功能

导出 WinRAR 设置的步骤。

❶ 打开 WinRAR。





注　意　事　项

软件并不会让选择导出文件的保存位置、文件名，导出的备份文件直接存放到安装文件夹 WinRAR 下的 Settings.reg 文件中，如果把 WinRAR 安装在系统分区中，那么必须在重装系统前把该 Settings.reg 转移到其他分区。

导入 WinRAR 设置的步骤。

❶ 打开 WinRAR。





注　意　事　项

如果转移了 Settings.reg 文件的保存位置，那就不能直接采用这种恢复方法了，但是可以直接双击该 Settings.reg 文件来进行恢复。

用这种备份方法所产生的 Settings.reg 文件其实和第一种直接备份注册表分支得到的文件内容是完全一样的。

技巧358　备份与还原系统字体

操作系统中的每一种字体都是一个字体文件，字体文件的存在保证了系统可以正常显示文字，所以做好系统字体的备份非常重要。

❶ 选择"开始"→"控制面板"命令。





❹ 选中需要备份的字体，右击并选择“复制”选项。

举 一 反 三

按下 Ctrl 键可同时选择多个文件。



❺ 将文件复制到备份文件夹中。

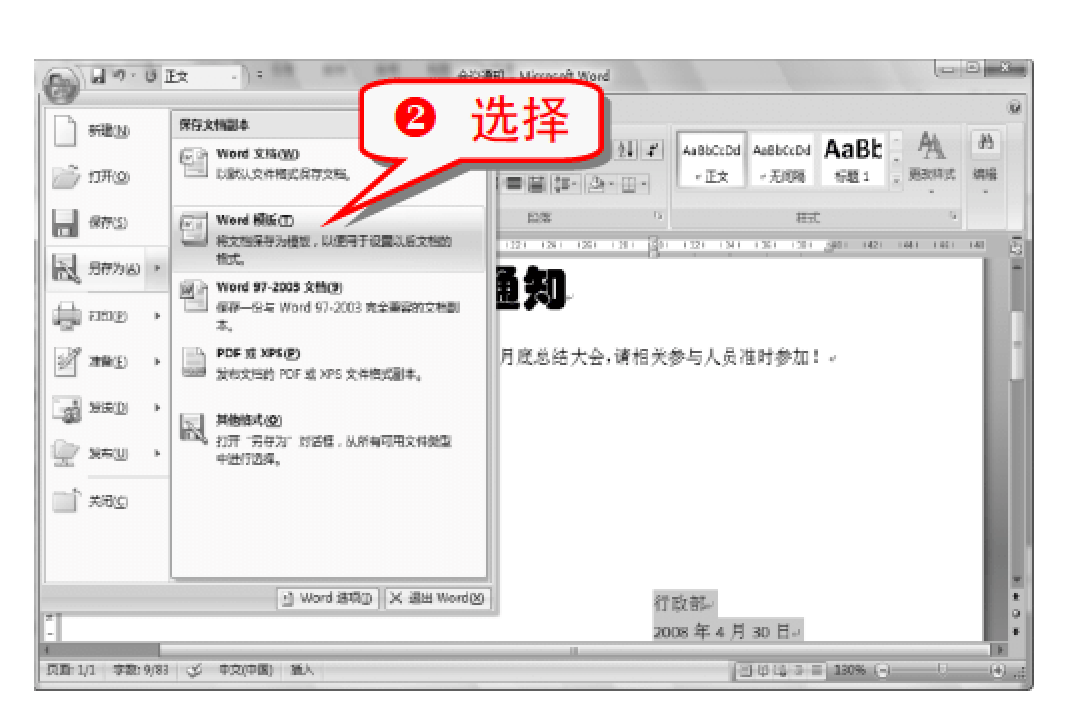
还原系统字体时只需将备份文件夹中的字体文件复制到原“字体”文件夹中即可。

技巧359　保存和调用 Word 2007 个性化模板

为某个文档定制好相关的样式以后，用户可将其保存到模板中，方便下次的调用。

(1) 保存为模板

❶ 在定制样式的文档中单击按钮，弹出下拉菜单。





(2) 调用模板

创建为模板后，假如需要再次创建样式相同的文档，可以直接调用已有的模板，具体步骤如下。

❶ 在“会议通知”文档中单击按钮，在弹出的菜单中选择“新建”命令。

❷ 在弹出的“新建文档”窗口中，单击左侧的“我的模板”按钮，弹出“新建”对话框。





专题十四　数据拯救与修复

内容导航

硬盘是保存数据的重要载体，由于硬盘数据量大和频繁使用的特点，经常会出现数据丢失的问题。如何找回丢失的数据成了普遍关心的问题。

热点快报

- 恢复被删除的文件
- 恢复格式化的文件
- 恢复损坏的文件
- 恢复误删 Office 文档
- 修复无效的子目录
- 恢复误删电子邮件

技巧360　EasyRecovery 数据恢复专家

EasyRecovery 是一款功能强大的数据恢复软件，可恢复因不慎操作引起的数据丢失，如硬盘误格式化，误删除分区和误删除文件等。

知　识　补　充

EasyRecovery 是著名数据恢复公司 Ontrack 旗下的一款产品。专业版包括了磁盘诊断、数据恢复、文件修复、E-mail 修复、19 个项目的各种数据文件修复和磁盘诊断方案等功能。



EasyRecovery 可以在以下几种情况下恢复数据。

- 主引导区(MBR)损坏。
- BIOS 参数块(BPB)损坏。
- 分区表损坏。
- 文件分配表(FAT)损坏。
- 主文件表(MFT)损坏。
- 根目录损坏。
- 病毒破坏。
- 误格式化或误删除分区。
- 误删除文件。
- 断电或瞬间电流冲击造成的数据毁坏。
- 程序的非正常操作或运行引起的数据损坏。
- 系统故障造成的数据毁坏。

专　家　坐　堂



EasyRecovery 在修复数据的时候是以“读取”的形式对需要修复的分区进行处理，不会将任何数据写入分区导致数据改变。另外 EasyRecovery 还包含了一个用来创建紧急启动软盘的使用程序，可在 Windows 无法启动的时候在 DOS 状态下进行数据恢复。

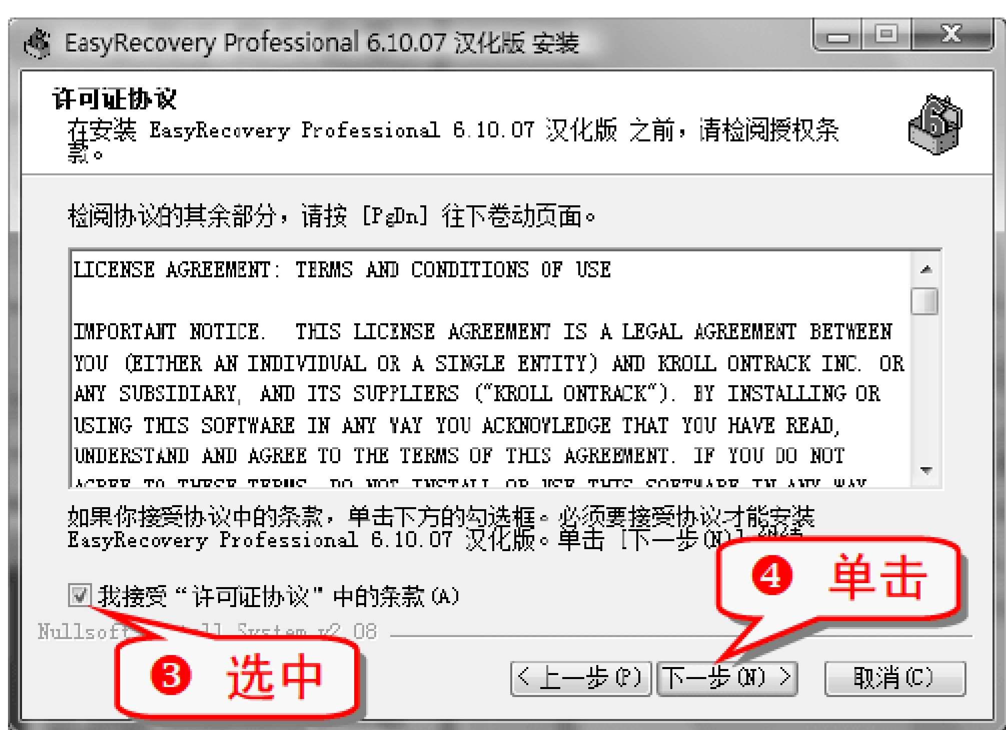
技巧361　EasyRecovery 的下载与安装

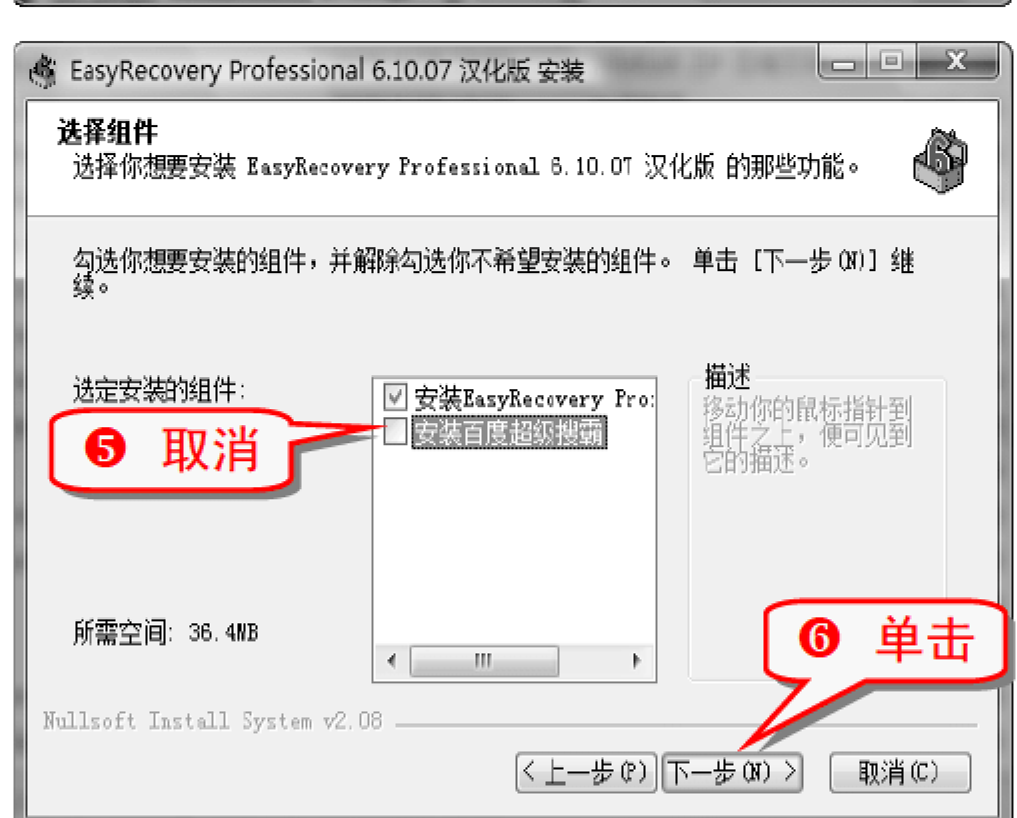
与其他工具软件一样，可以在网上搜索并下载到 EasyRecovery。

❶ 下载完成后，双击其安装程序，在弹出的语言选择下拉列表中选择 Chinese(Simplified)，单击 OK 按钮。



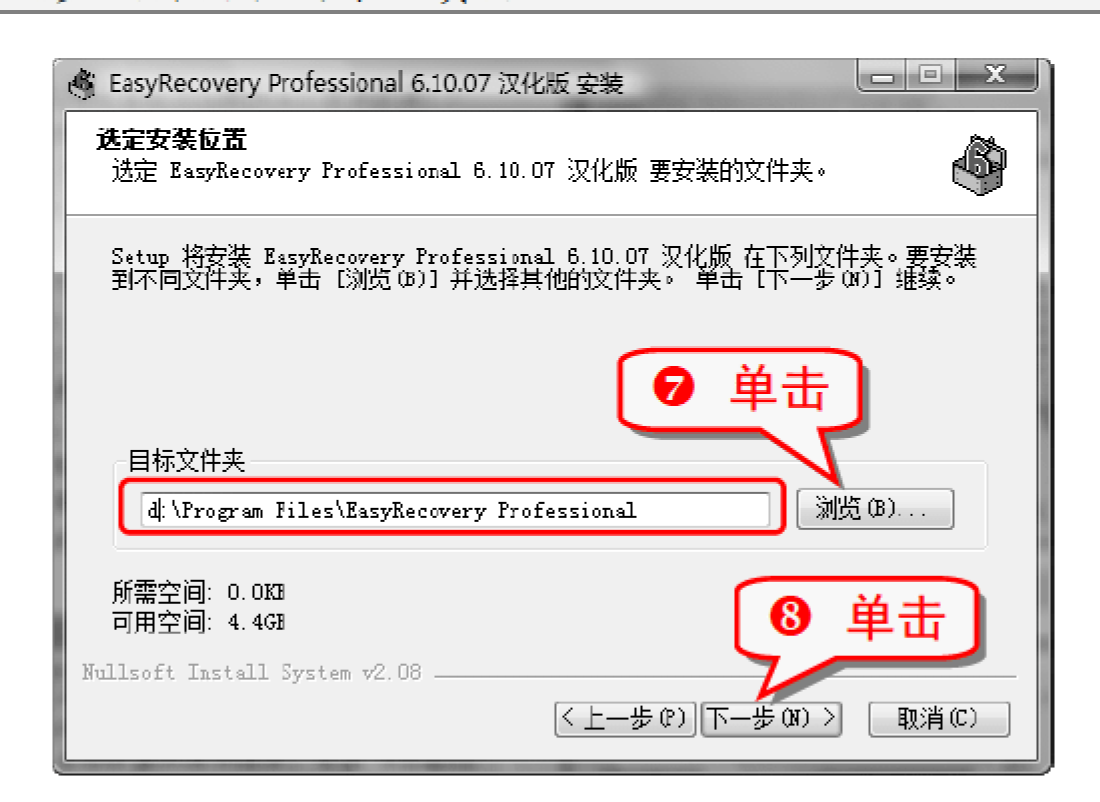


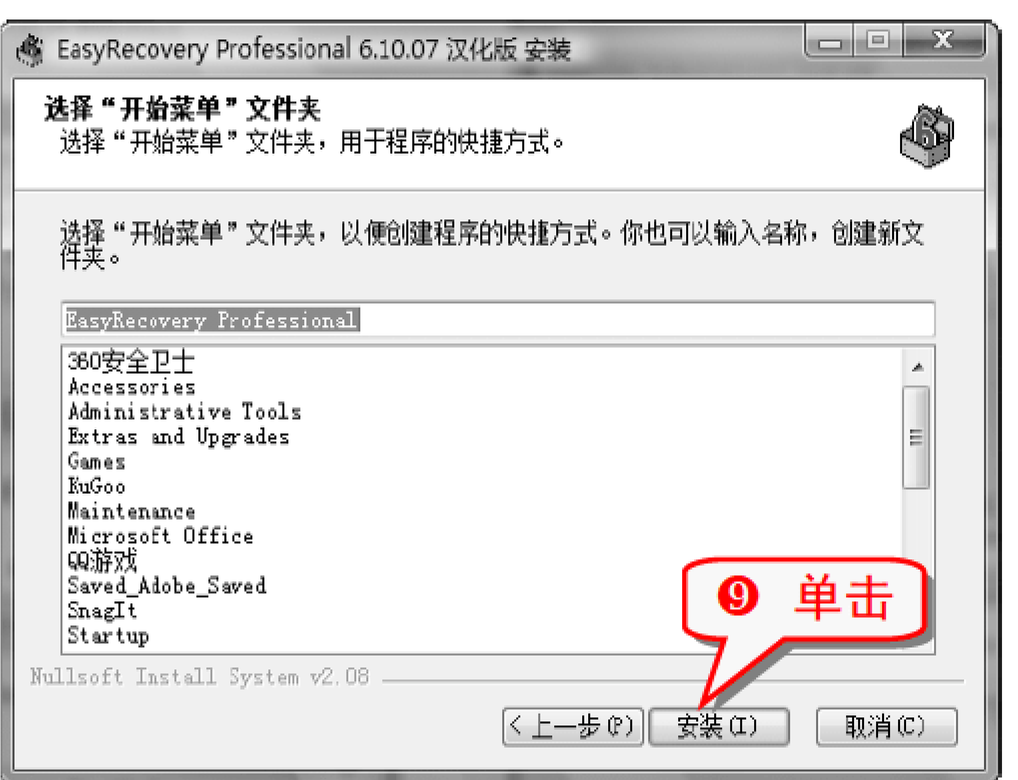


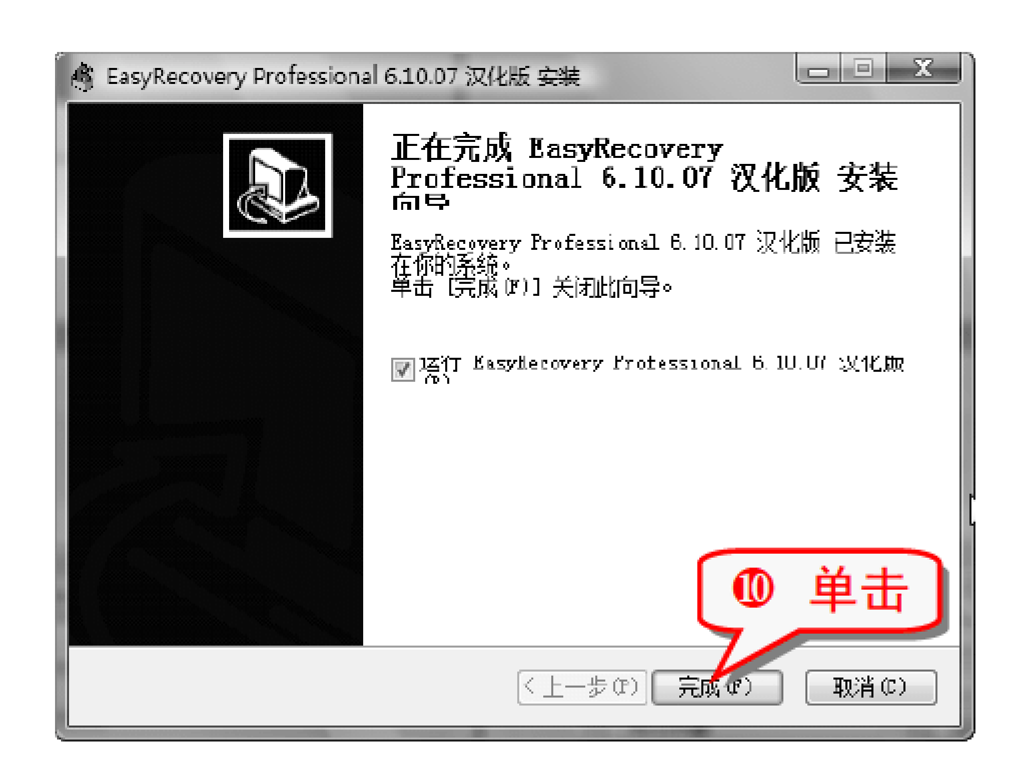


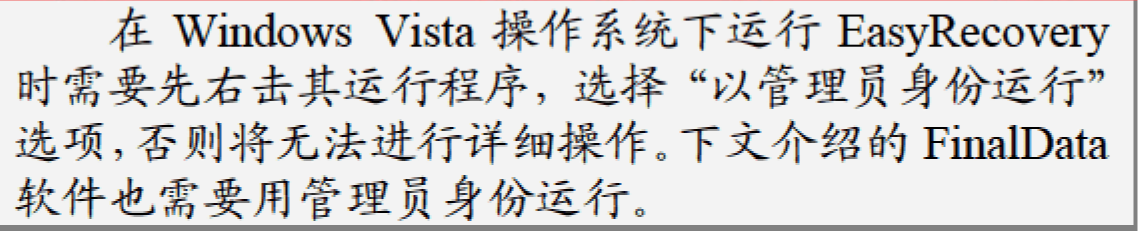
注 意 事 项

注意不能取消选中“安装 EasyRecovery”复选框，否则 EasyRecovery 将不被安装。“百度超级搜霸”是一款免费的 IE 浏览器工具栏，不建议用户安装，安装过多插件会占用系统资源。









在 Windows Vista 操作系统下运行 EasyRecovery 时需要先右击其运行程序，选择“以管理员身份运行”选项，否则将无法进行详细操作。下文介绍的 FinalData 软件也需要用管理员身份运行。

技巧362 EasyRecovery 的数据拯救与修复功能

打开 EasyRecovery，可发现在其界面右侧有六个选



项，代表了六个 EasyRecovery 的主要功能。




专 家 坐 堂

EasyRecovery 功能非常齐全、强大，了解其功能有助于用户更好地利用 EasyRecovery 进行数据恢复。

(1) 磁盘诊断

磁盘诊断又分了六个小功能模块，具体如下。

- 驱动器测试：主要用于检测硬件存在的潜在问题。
- SWART 测试：磁盘检测功能，主要用于检测、监视并报告磁盘数据方面存在的问题。
- 空间管理器：可查看每个磁盘驱动器空间的使用情况。
- 跳线查看：查找 IDE/ATA 磁盘驱动器的跳线设置。
- 分区测试：主要用于分析现有的文件系统结构。
- 数据顾问：可用向导的方式创建 16 位下分析磁盘的启动软盘。

(2) 数据恢复

数据恢复是 EasyRecovery 最核心的一个功能模块，具体用途如下。

- 高级恢复：可自定义数据恢复。
- 删除恢复：主要用于查找并恢复被删除的文件。
- 格式化恢复：主要用于查找并恢复因格式化而丢失的数据。
- Raw 恢复：主要用于恢复受损分区和文件目录中的数据。
- 继续恢复：继续上一次没有完成的数据恢复。
- 紧急启动盘：可创建自引导紧急启动盘，内含恢复工具，在 Windows 不能正常启动的情况下进行数据修复。



(3) 文件修复

与文件恢复找回丢失的文件不同，文件修复主要用于用户被破坏文件的还原。

- Access 文件修复：主要用于修复损坏的 Access 数据库。
- Excel 文件修复：主要用于修复损坏的 Excel 表格。
- PowerPoint 文件修复：主要用于修复损坏的 PowerPoint 演示文稿。
- Word 文件修复：主要用于修复损坏的 Word 文档。
- Zip 文件修复：主要用于修复损坏的 Zip 文件。

(4) Email 修复

此模块主要用于邮件的修复。

- Outlook 修复：主要用以修复损坏的 Outlook 文件。
- OutlookExpress 修复：主要用以修复损坏的 OutlookExpress 文件。

(5) 软件升级

此模块用以获得 EasyRecovery 产品最新的信息。

- 产品新闻：检查可用的新产品组件。
- 快速升级：可在线获得最新的软件更新。

(6) 救援中心

此模块是 EasyRecovery 为用户提供的其他服务项目。

- 救援中心信息：为用户提供信息与技术支持。
- 远程数据恢复：可通过调制解调器或者 Internet 进行数据恢复。
- 实验室数据恢复：主要用于从物理损坏的磁盘上恢复数据。
- 超值产品：提供各种数据恢复解决方案的报价。




在“属性设置”中可详细设置各模块的相关选项；在“快速启动”中可自定义快速启动菜单。

技巧363　EasyRecovery 恢复被删除文件

在使用电脑的过程中，难免会误删除文件，或者将文件彻底删除了以后又想找回来，此时可采用 EasyRecovery 数据恢复中的删除恢复功能来恢复数据。

(1) 扫描被删除文件





知 识 补 充

此处选择的分区是被删除文件所在分区，扫描的文件类型默认选择为所有文件，单击下拉箭头可详细选择 Office、网页、图片和源代码等各类型文件。



举 一 反 三

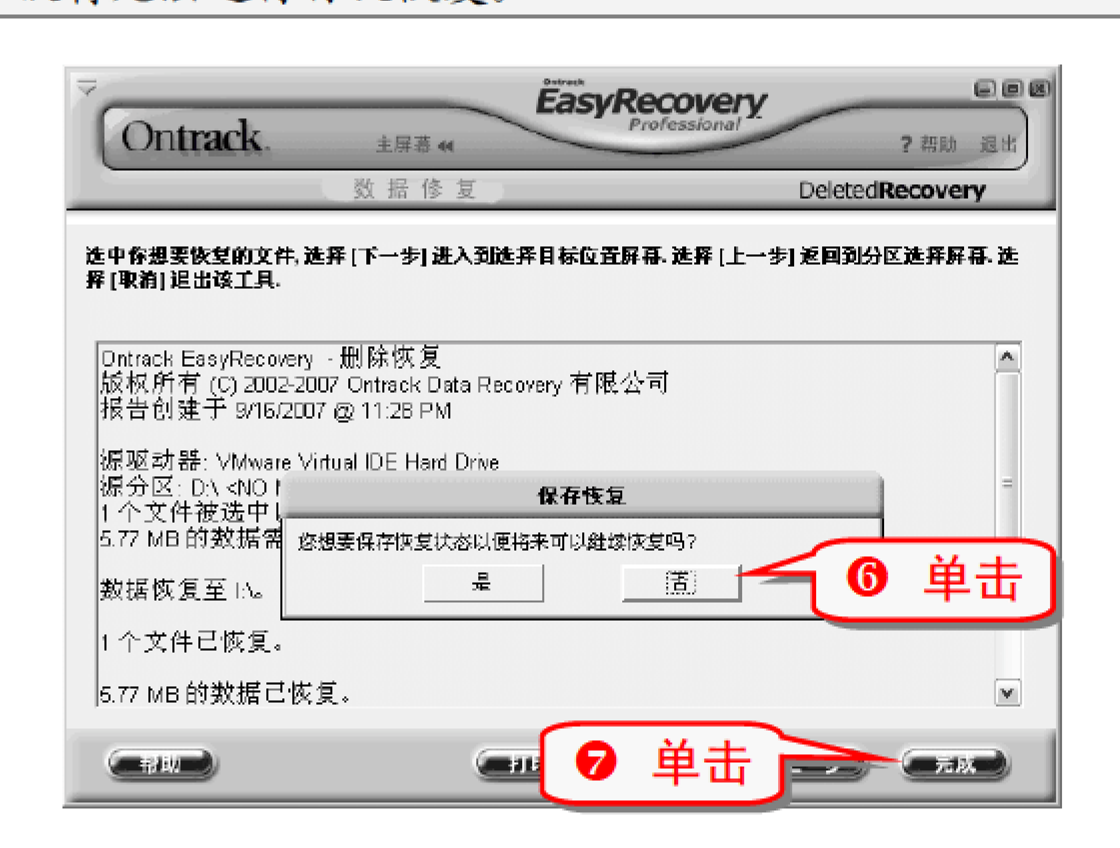
单击“过滤器选项”按钮可将扫描结果进行过滤，单击“查找”按钮可在众多被扫描出来的文件中快速查找需要的文件。

(2) 恢复被删除文件



注 意 事 项

选择保存恢复文件的位置时，不能选择被删除文件所在的分区。如果选择保存在原位置，一旦恢复错误将无法进行再次恢复。




举 一 反 三

如果选择“是”可在下次打开 EasyRecovery 时使用“继续恢复”功能继续未完成的数据恢复。此处数据恢复已经完成，所以选择“否”。

在保存恢复文件的位置打开文件即可查看恢复后的文件，但是恢复后的文件有可能已被损坏，此时可采用文件修复功能修复相关文件。

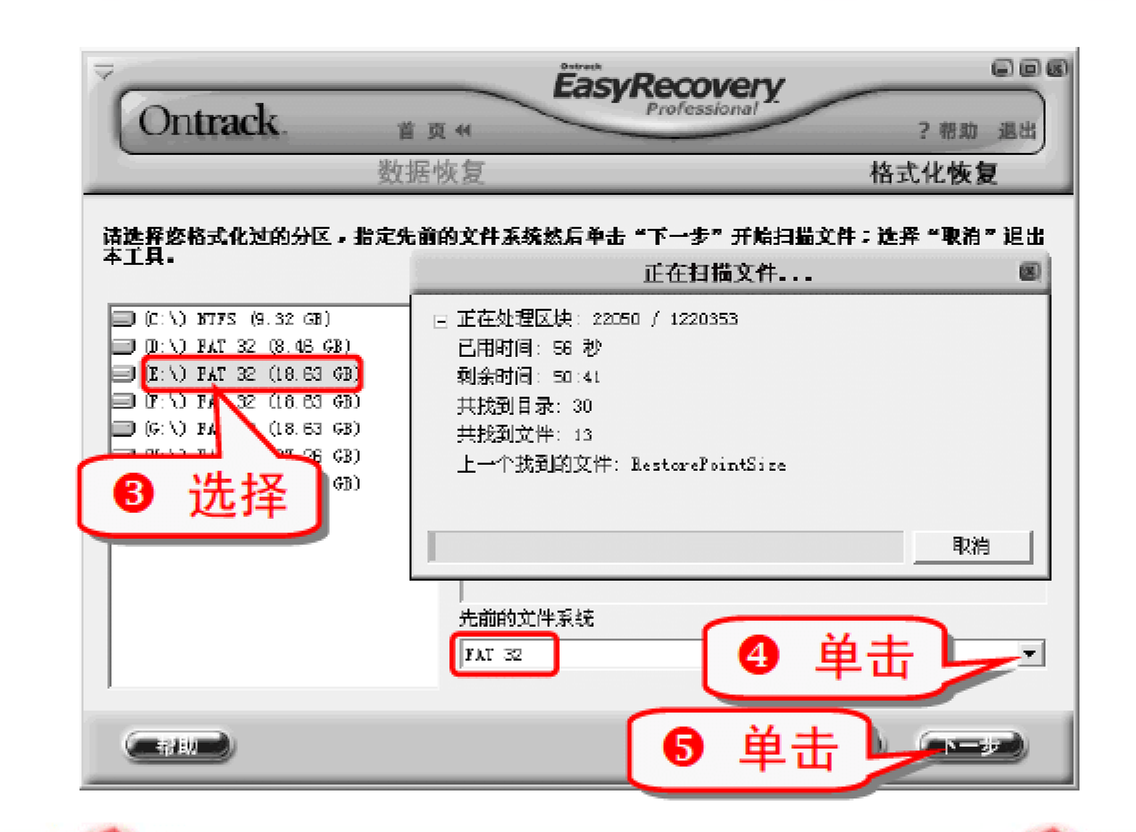
技巧364 EasyRecovery 恢复格式化文件

因分区被格式化而丢失的文件可采用数据恢复中的格式化恢复功能来进行恢复。

(1) 找到因格式化而丢失的文件

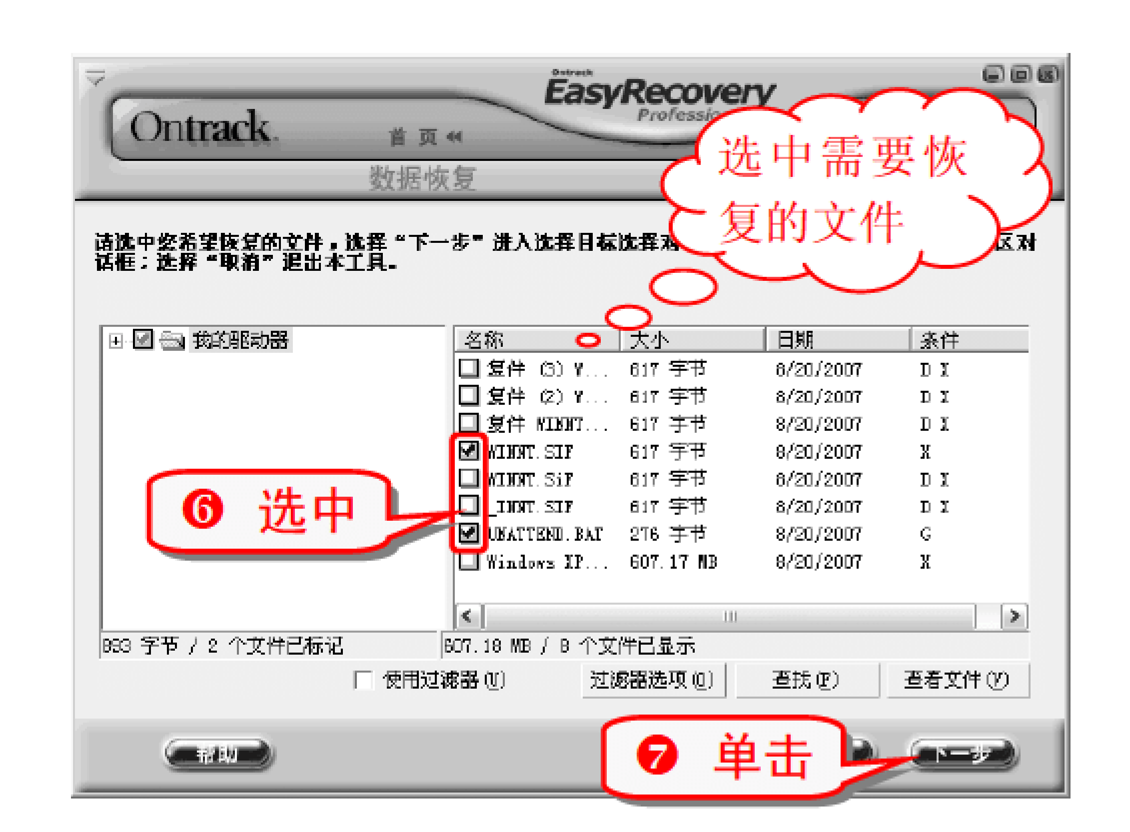






注　意　事　项

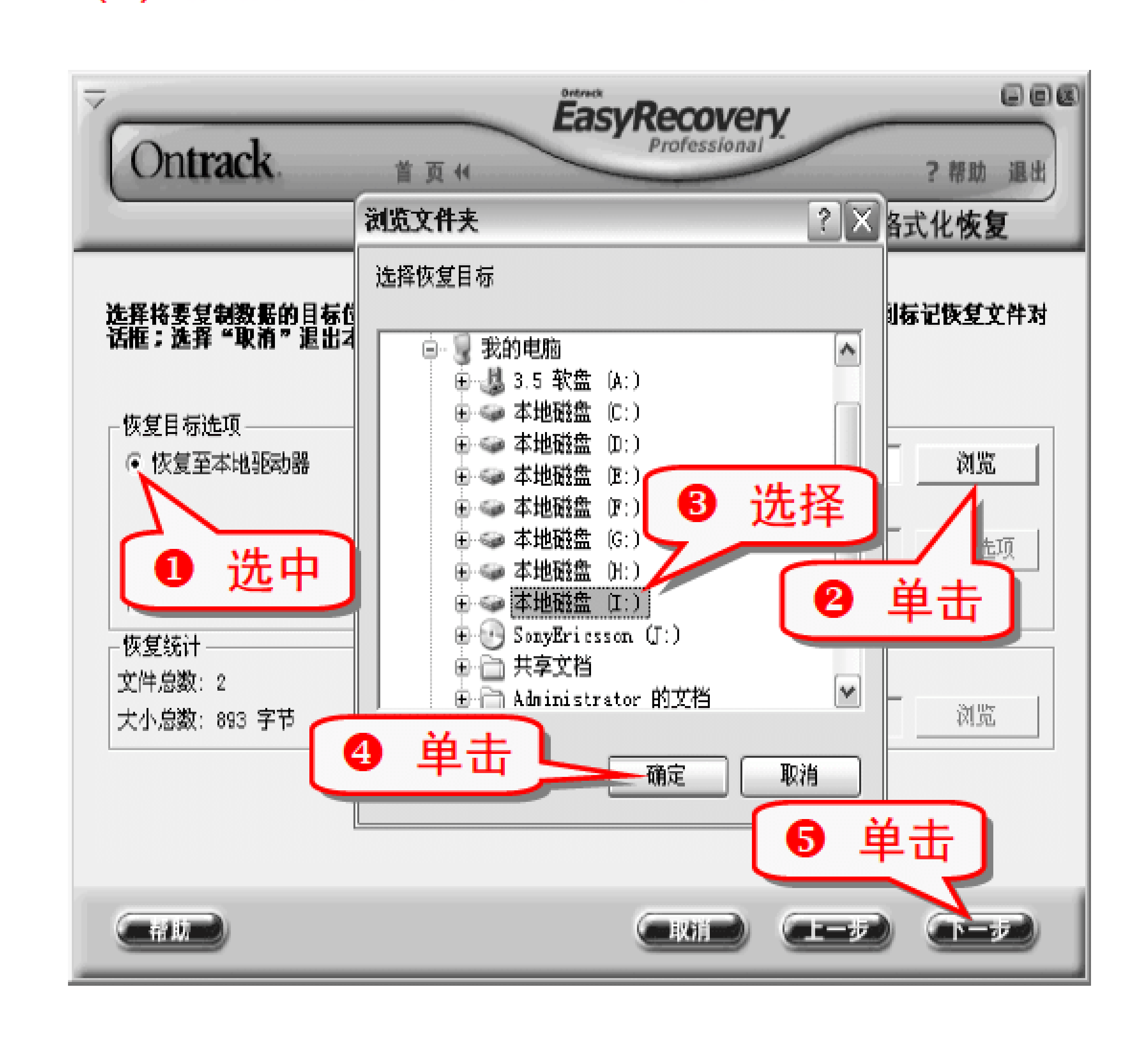
此处选择的是被格式化的分区，文件系统的选择必须与被格式化前的分区文件系统格式一致。

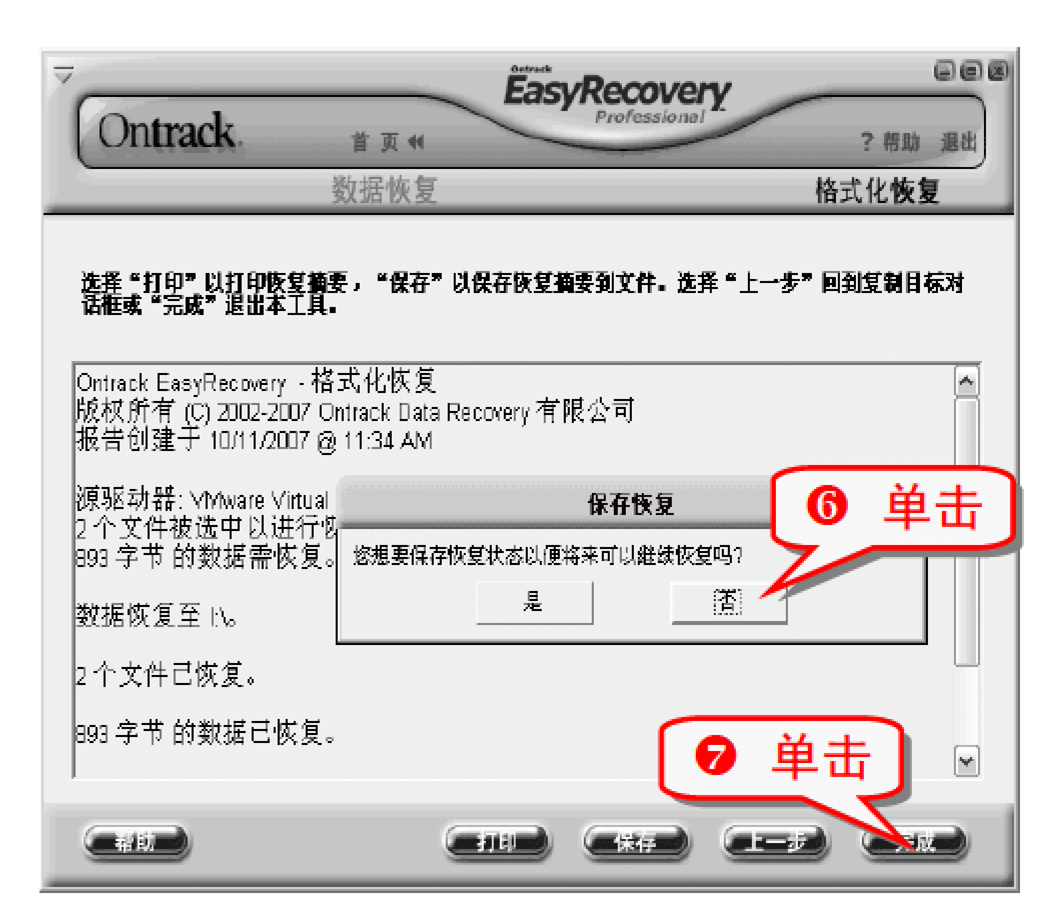


知　识　补　充

单击“查看文件”按钮可查看被选中文件的详细内容，以确定此文件是否需要被恢复。

(2) 恢复因格式化而丢失的文件



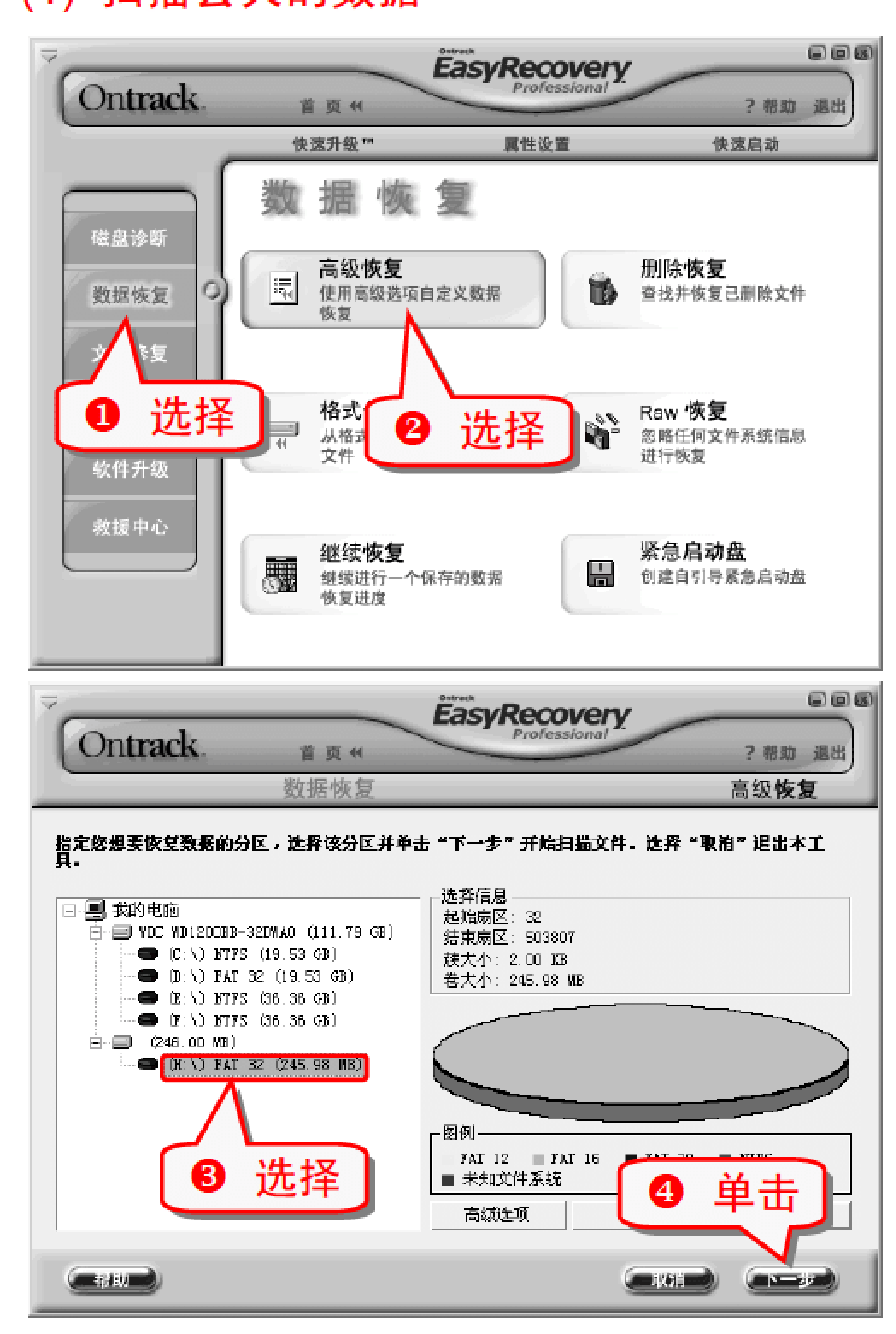


技巧365　EasyRecovery 高级恢复丢失数据

当采用删除恢复和格式化恢复都无法成功找回丢失的数据时，可采取高级恢复从损坏分区中扫描并恢复数据。

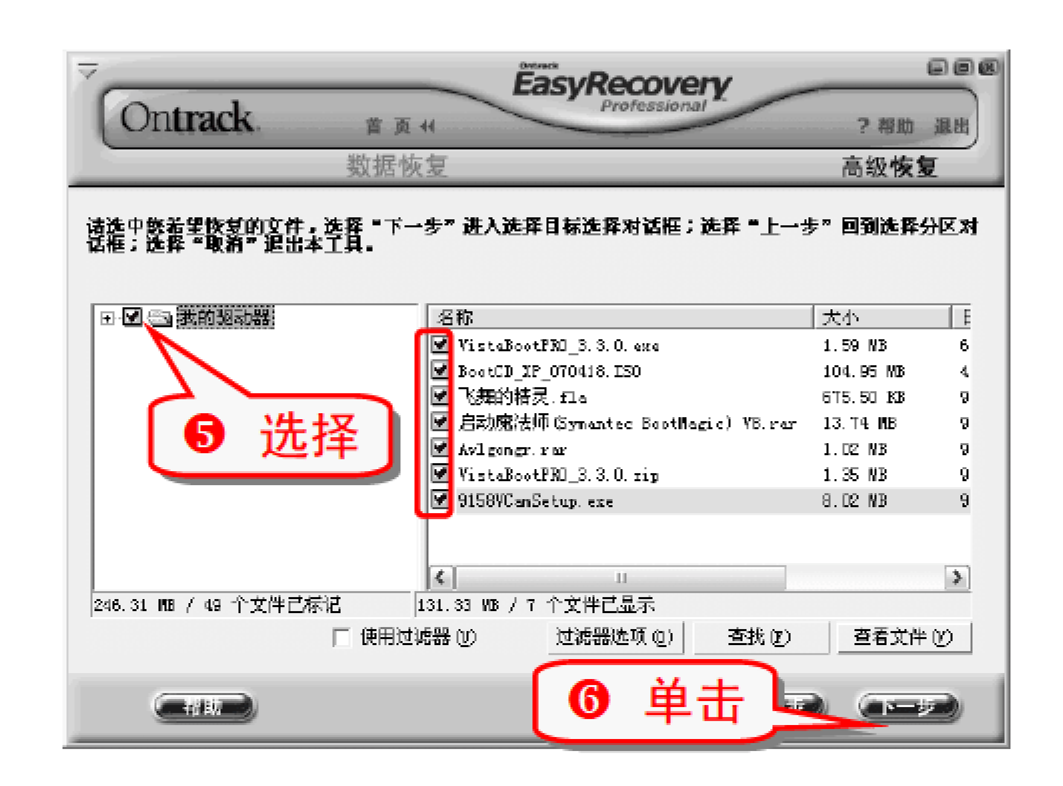
高级恢复采用文件标识搜索，可从头搜索分区的所有簇，不依赖于分区文件系统结构，所以只要是存在于分区中的数据块都有可能被搜索到，经过判断后将需要的文件进行恢复。

(1) 扫描丢失的数据



专 家 坐 堂

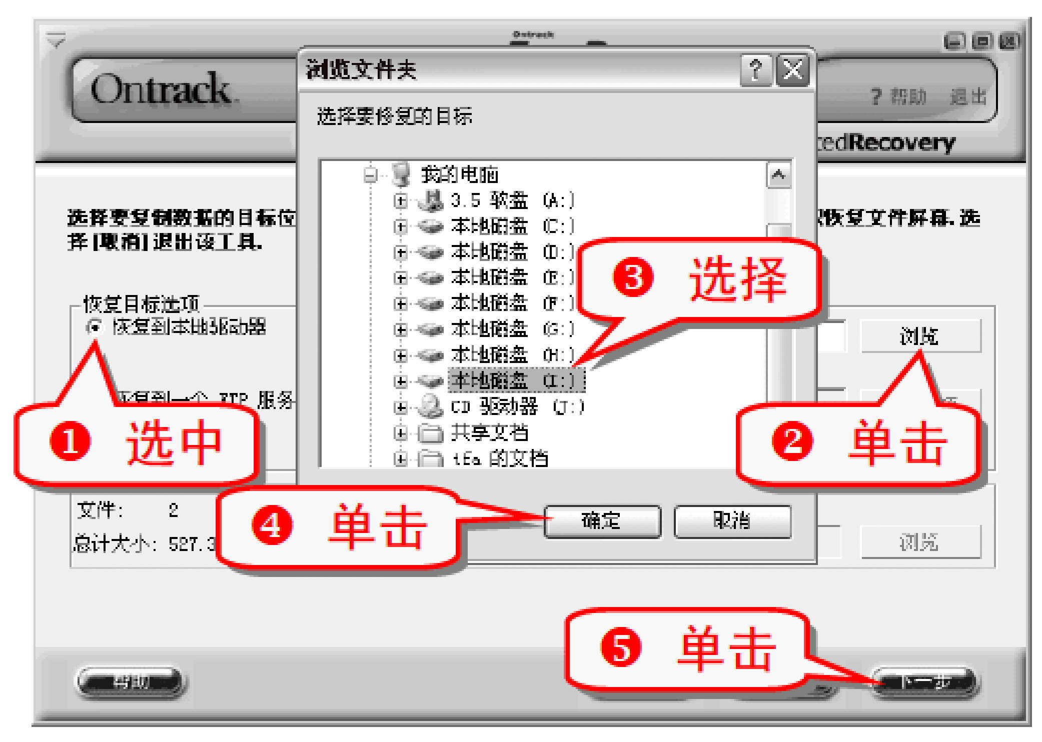
如果扫描分区的容量过大，会花费较长时间，可在进行扫描前在“高级选项”的“分区信息”中设置需要扫描的起始扇区和结束扇区，缩小扫描范围。

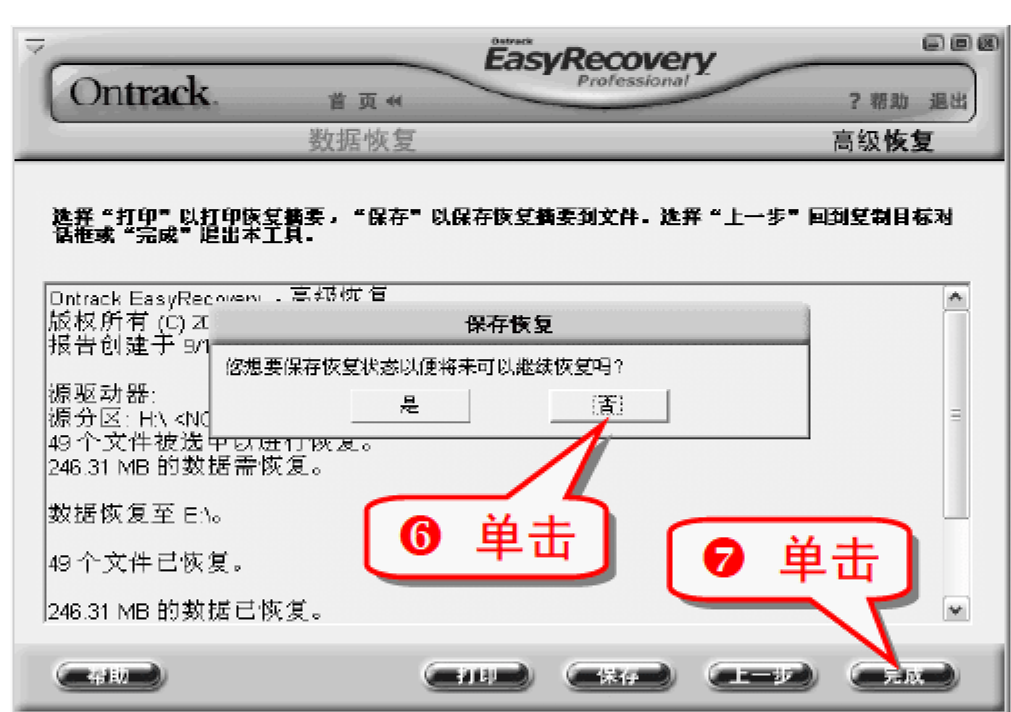


注 意 事 项

选择“我的驱动器”将选中所有的文件进行恢复，如果只需恢复某些文件，可在右侧窗格进行对应的选择。

(2) 恢复丢失的数据





举 一 反 三

如果需要保存恢复，在下次启动 EasyRecovery 时继续进行未完成的数据恢复，可选择“是”，在弹出的对话框中指定保存数据的位置和名称，单击“确定”按钮。下次只需选择刚才保存的文件即可进行继续恢复。

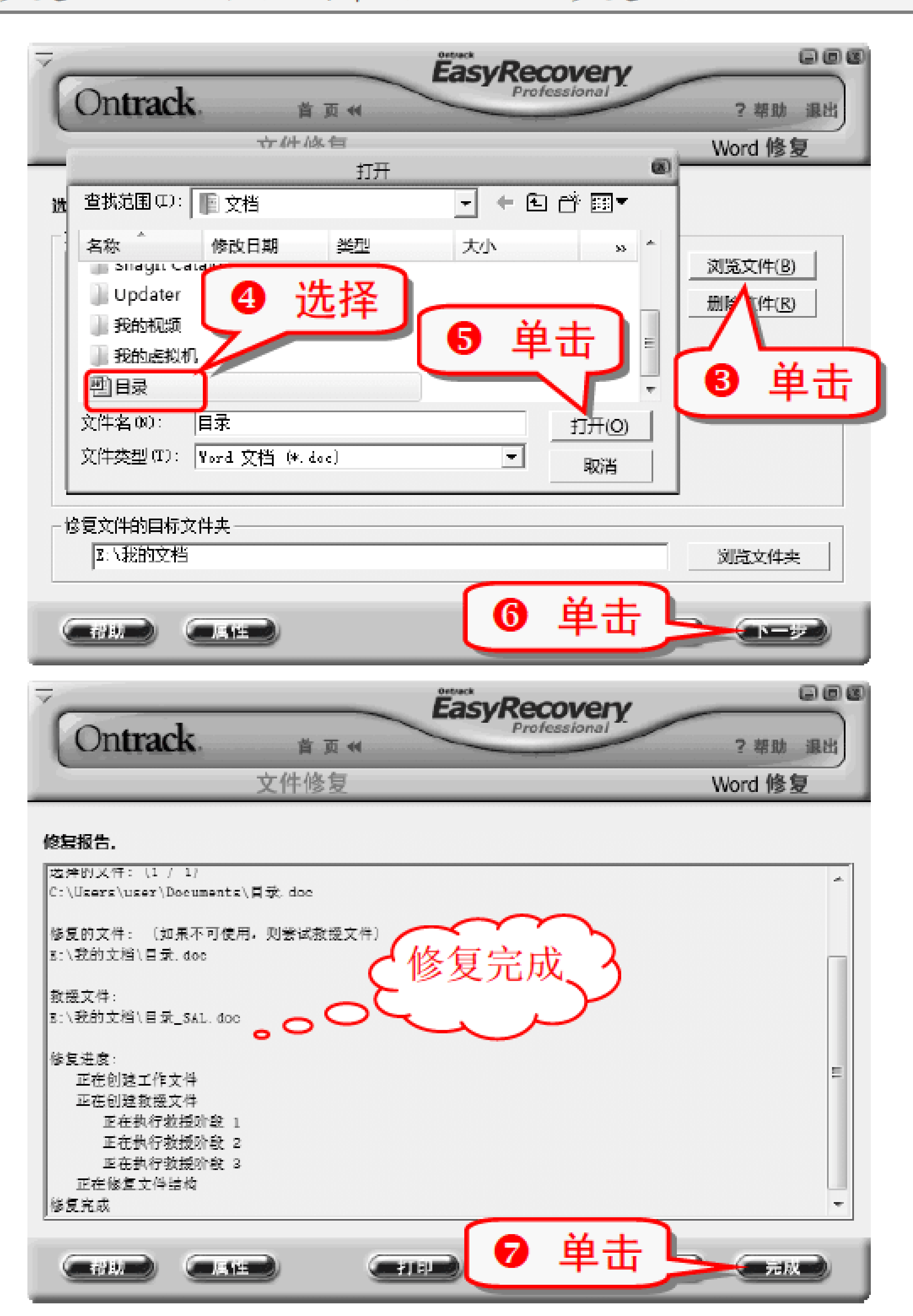
技巧366 EasyRecovery 修复损坏的文件

文件在使用的过程中因为各种原因，有可能被损坏，另外被恢复的数据也有可能不慎受损，此时可采用文件修复来进行相关文件数据的修复。



举 一 反 三

根据被修复的文件类型进行对应选择，例如需要修复 Word 文档，则单击“Word 修复”。






举　一　反　三


E-mail 修复中的 Outlook 文件与 OutlookExpress 文件修复步骤与 Word 文件一样。

技巧367　FinalData 数据恢复好帮手

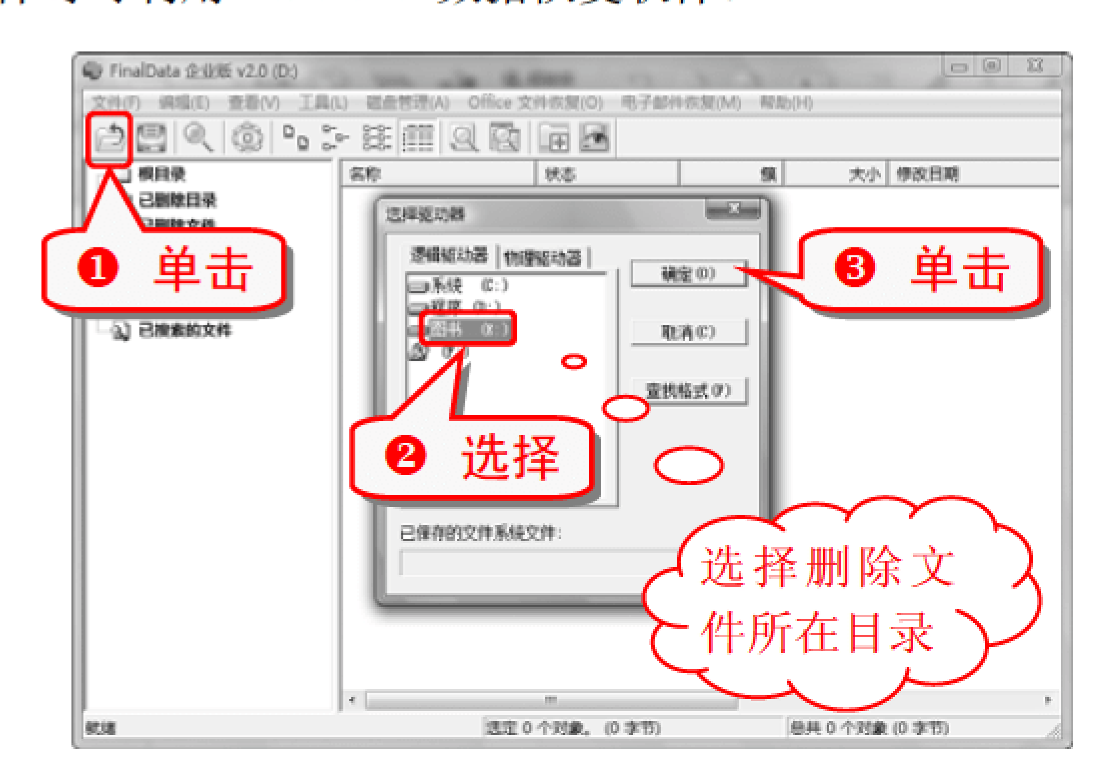
FinalData 也是一款优秀的数据恢复软件，其功能非常强大，且操作很简单。

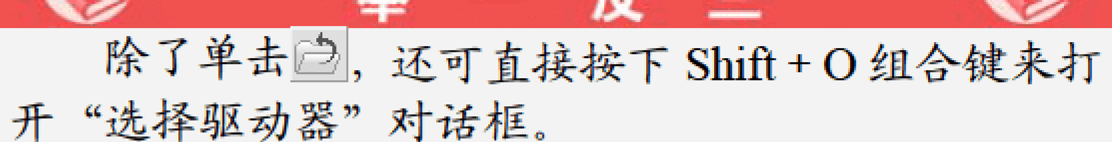
FinalData 可以恢复的主要内容有：

- 丢失的数据。
- 主引导记录(MBR)。
- DOS 引导扇区(DBR)。
- FAT 表等数据信息。

技巧368　FinalData 恢复误删除文件

通常被删除的文件是暂时存放在“回收站”中，而没有直接被删除。但是按下 Shift+Delete 组合键删除文件时可将文件彻底从电脑中删除。此时想恢复被彻底删除的文件时可利用 FinalData 数据恢复软件。



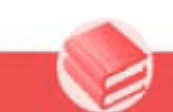

举　一　反　三

除了单击[图标]，还可直接按下 Shift + O 组合键来打开“选择驱动器”对话框。

❹ 在扫描结果中找到被删除的文件，右击需要修复的文件。





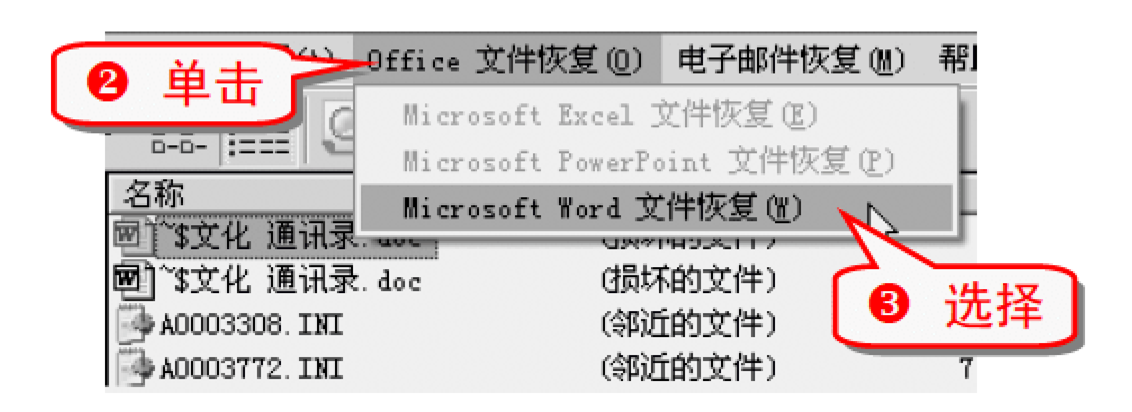
举　一　反　三


在“回收站”中的文件也可进行恢复，进入“回收站”，右击需要恢复的文件，选择“还原”即可。

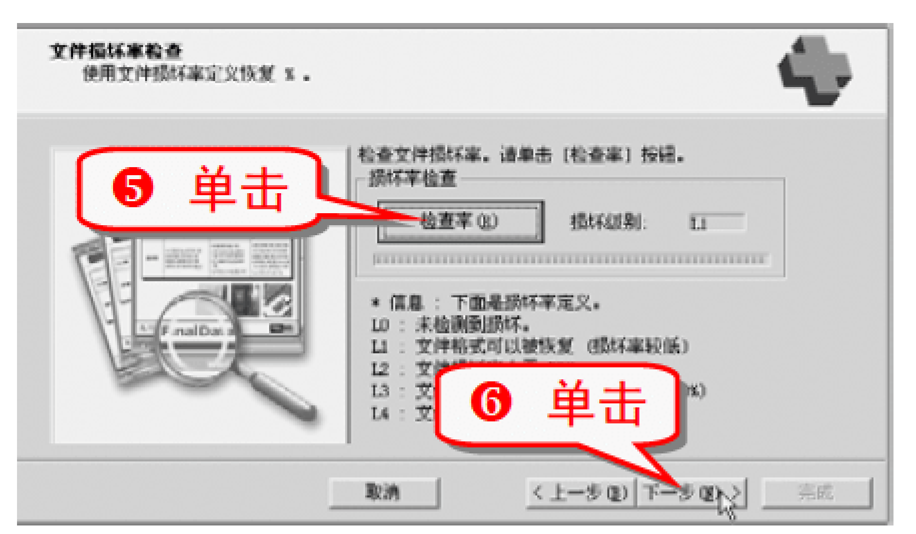
技巧369　FinalData 恢复误删除 Office 文档

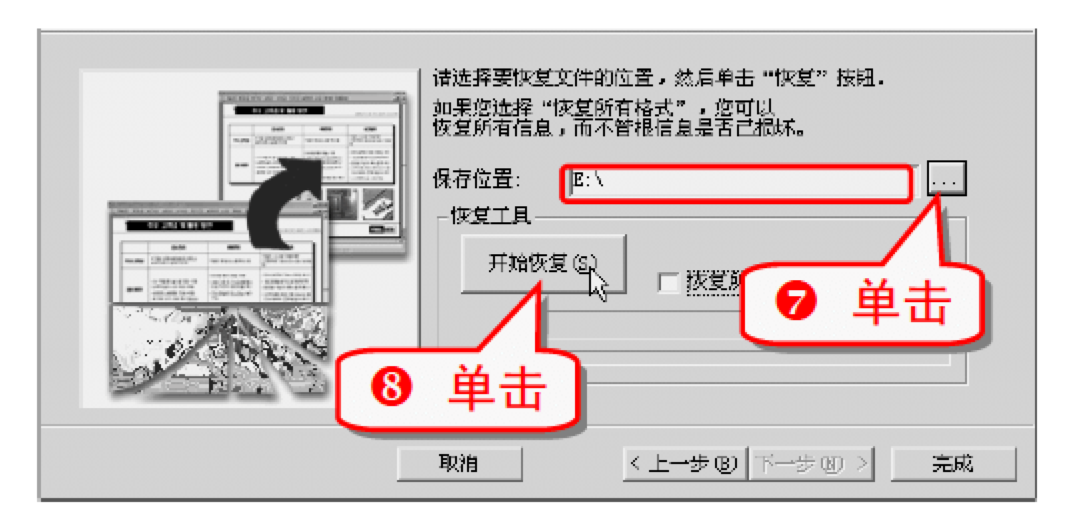
利用 FinalData 同样可以恢复被误删除的 Office 文档，且操作十分简单。

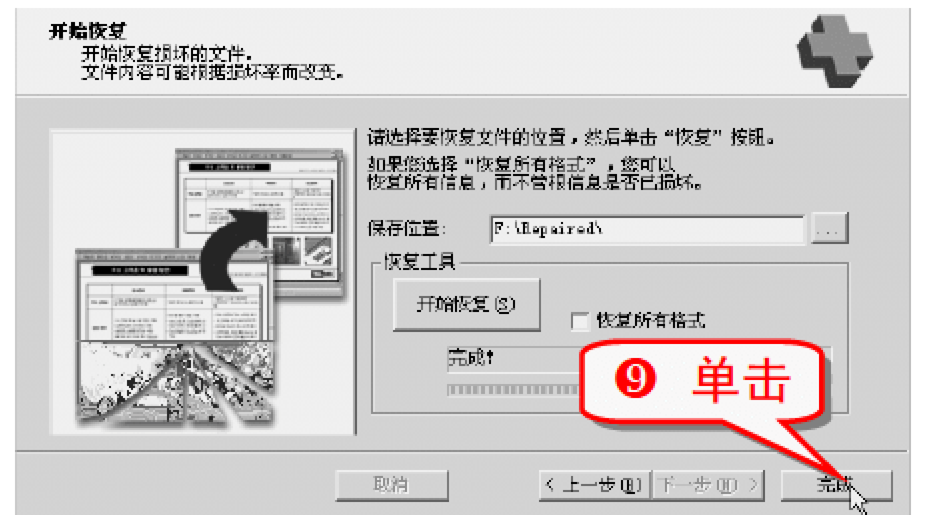
❶ 按照上面的方法扫描被删除文件所在的分区，找到被删除的文件并选择需要被修复的文件。









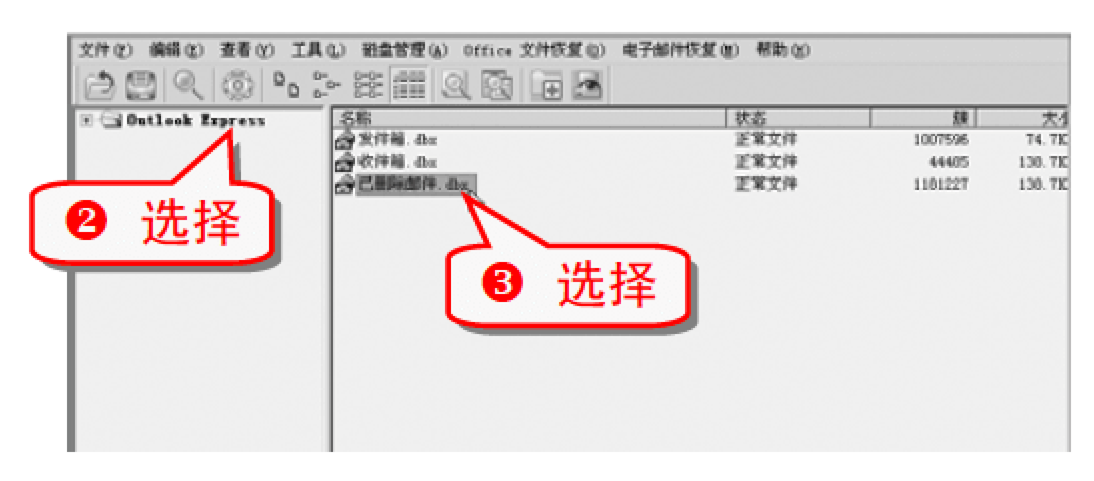


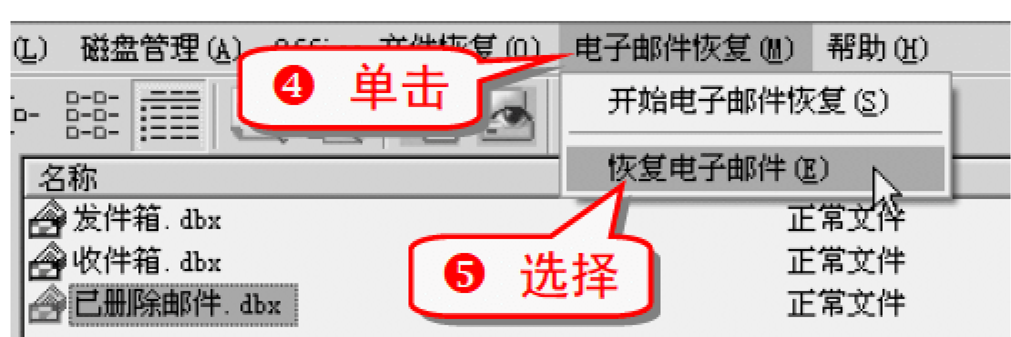
注　意　事　项

与 EasyRecovery 一样，利用 FinalData 恢复数据时，恢复文件的保存位置不能选择被恢复文件的原位置。

技巧370　FinalData 恢复误删除电子邮件

❶ 按照上面的方法扫描被删除电子邮件所在的分区。







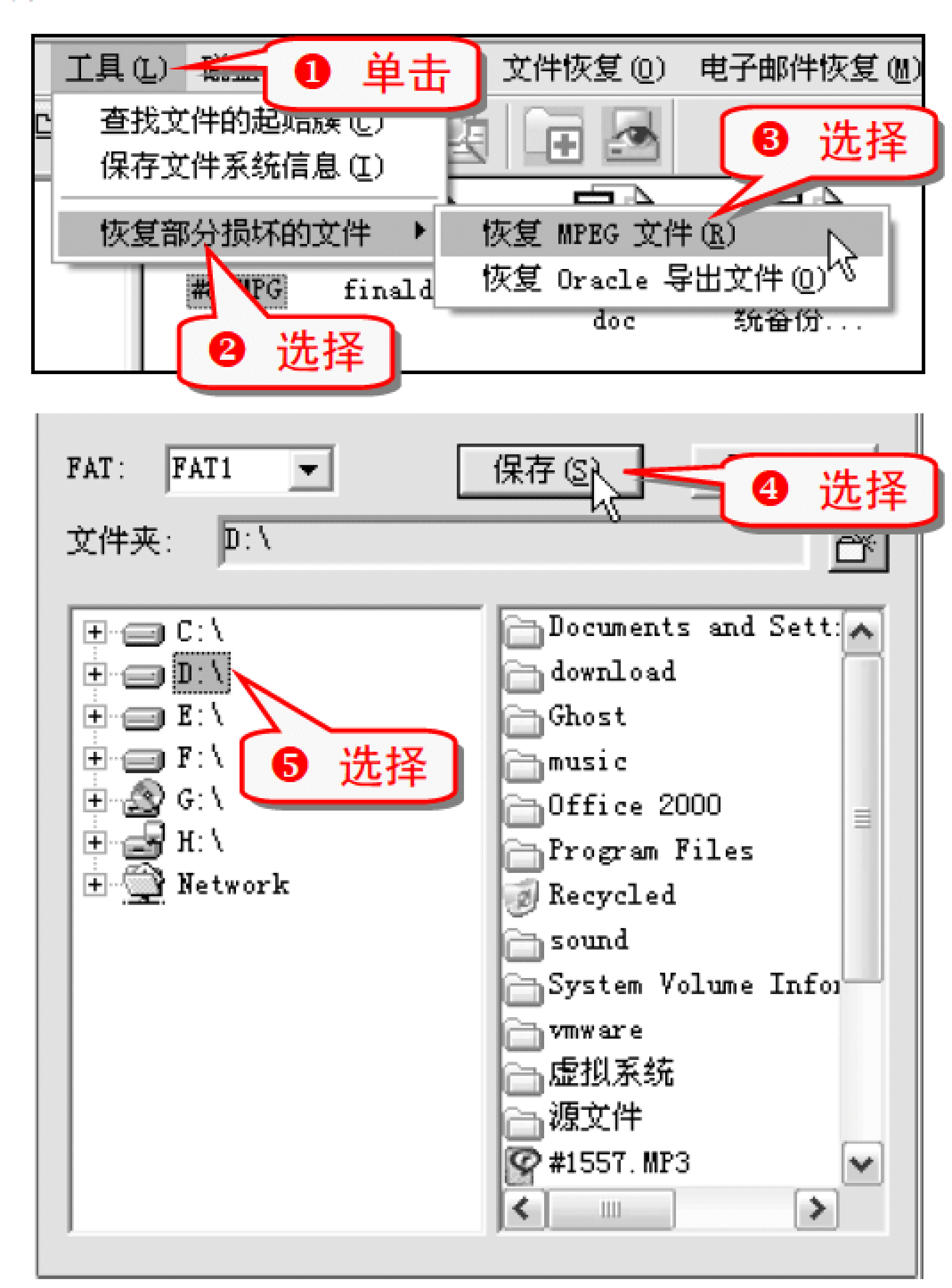


专　家　坐　堂

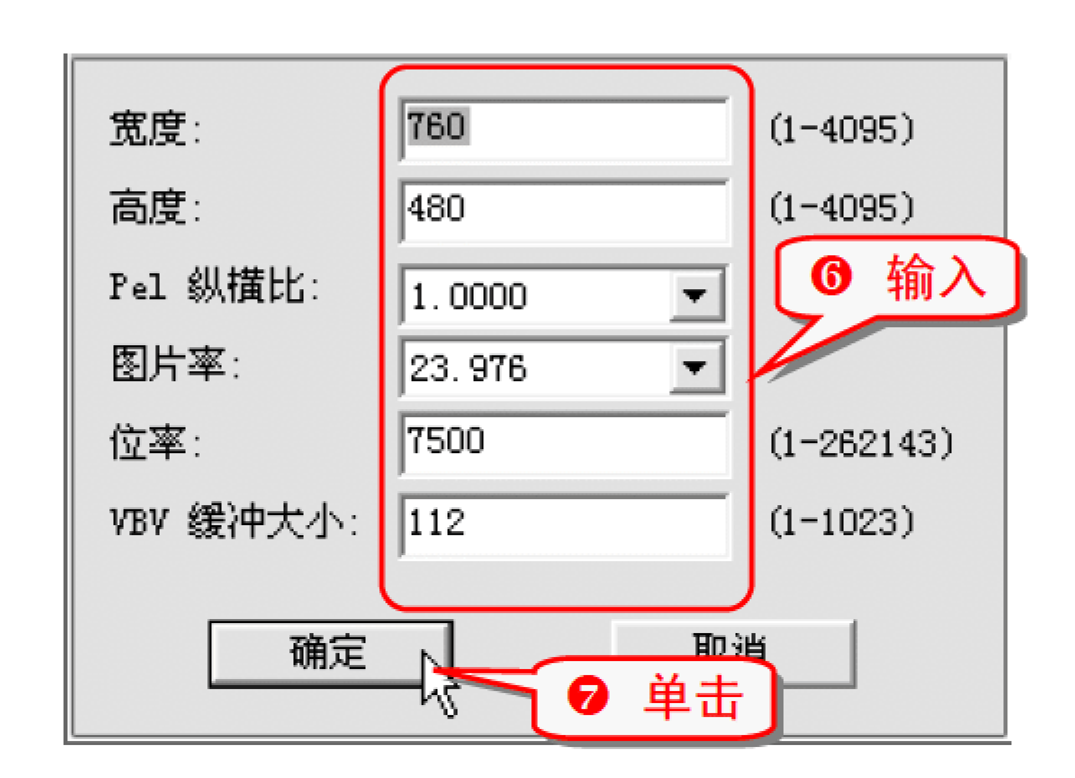
进入保存恢复文件的文件夹，找到后缀名为 eml 的文件即可打开恢复的邮件。

技巧371　FinalData 恢复损坏文件

利用 FinalData 可恢复损坏的 MPEG 和 Oracle 导出文件。







注　意　事　项

此处恢复的是损坏的 MPEG 图片文件，用户可根据不同图片进行不同的宽度、高度等项的设置。

技巧372　用 CHKDSK/F 命令找回丢失簇

电脑在运行时，由于各种意外会导致硬盘文件目录表(FDT)或者文件分配表(FAT)出错，导致文件内容丢失。簇的丢失就是其中一类情况。

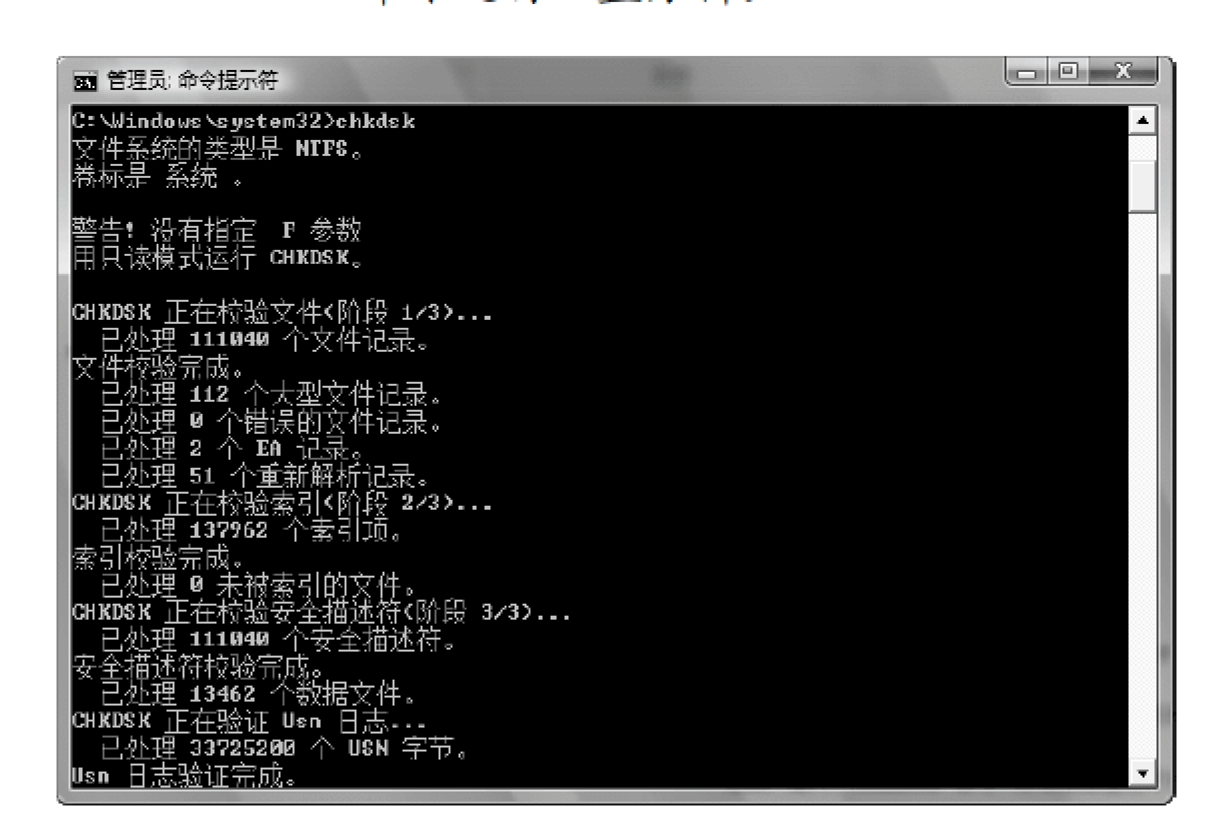
在进行磁盘写入操作时，当簇被分配给文件并写上数据时，文件分配表(FAT)也会随之更新，此时如果在 FAT 项已经建立起来，而对应的“开始簇”还没有写到文件目录表(FDT)的情况下发生意外，例如意外关机或者系统故障，就会发生簇丢失。

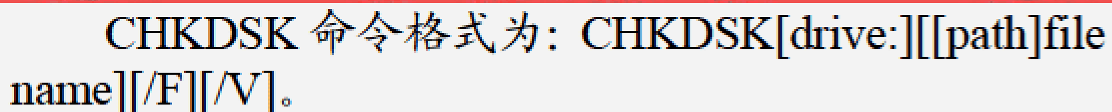
通俗地讲，丢失的簇就相当于一个没有名字的文件。

❶ 选择“开始”→“所有程序”→“附件”命令。



❹ 在弹出的“管理员：命令提示符”窗口中输入 CHKDSK/F 命令进行磁盘分析。





CHKDSK 命令格式为：CHKDSK[drive:][[path]file name][/F][/V]。

[drive:][path]：指定被检测的驱动器和路径名。

file name：指定被检测和修复的文件名。

/F：修复磁盘错误。

/V：显示磁盘上的所有路径和文件名。

技巧373　修复无效子目录

一个子目录必须含有“.”和“..”两个目录项，当不慎丢失这两项时，CHKDSK 检测时会认为目录无效，并且提示下面信息：

> 无效子目录项
> 转换成文件吗(Y/N)?

此时建议用户选择 N 取消文件转换，因为如果选择 Y，CHKKSK 会将无效子目录转换为 FILExxxx.CHK 文件，而该子目录下的文件都成了只有 FAT 链而在 FDT 中没有文件目录项的文件，这将再次造成文件簇的丢失。

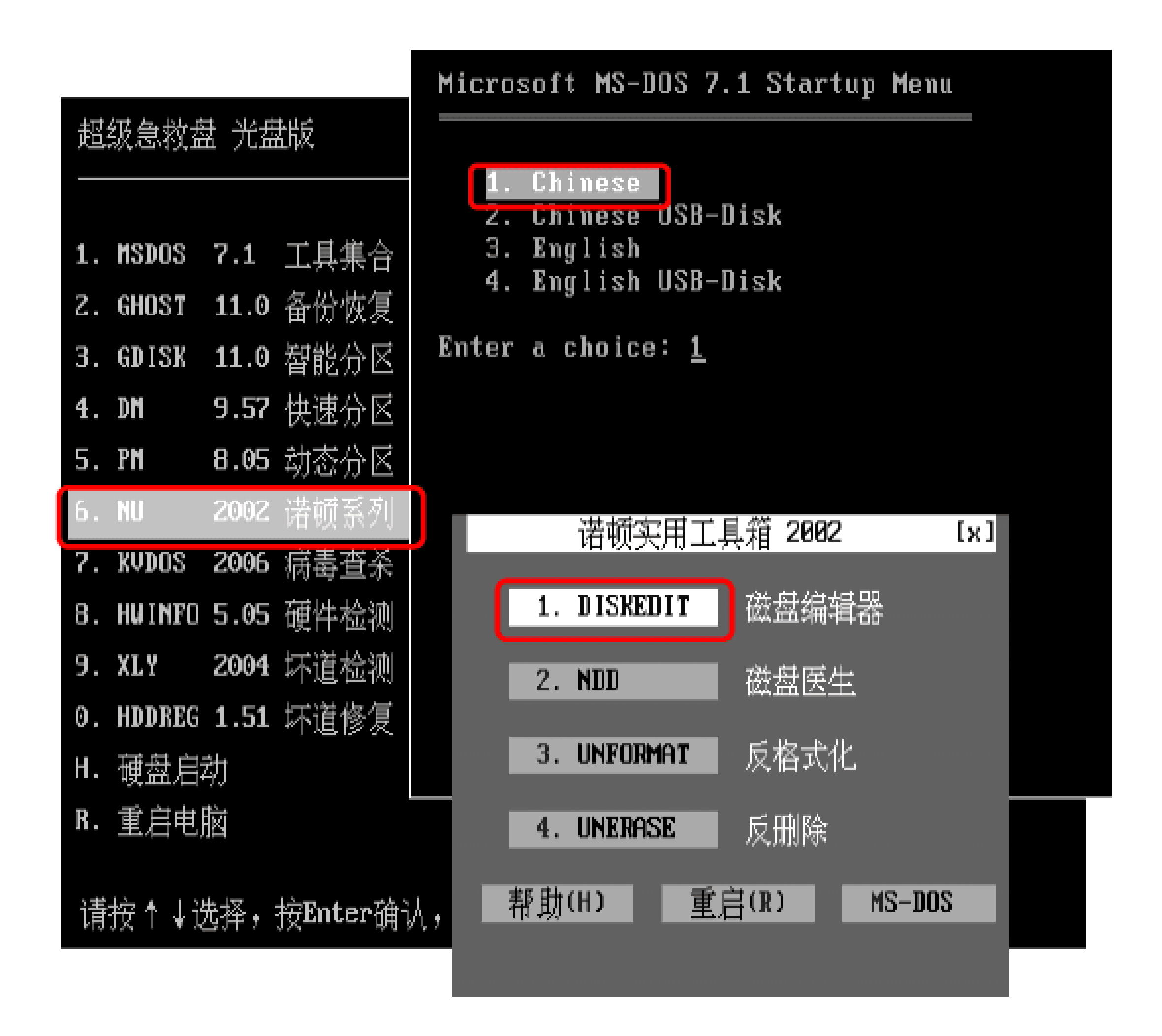
当子目录无效时，可采用 DEBUG 和 Disk Editor 来进行修复，例如 Norton 8.0 的 Disk Editor(超级急救工具盘)。

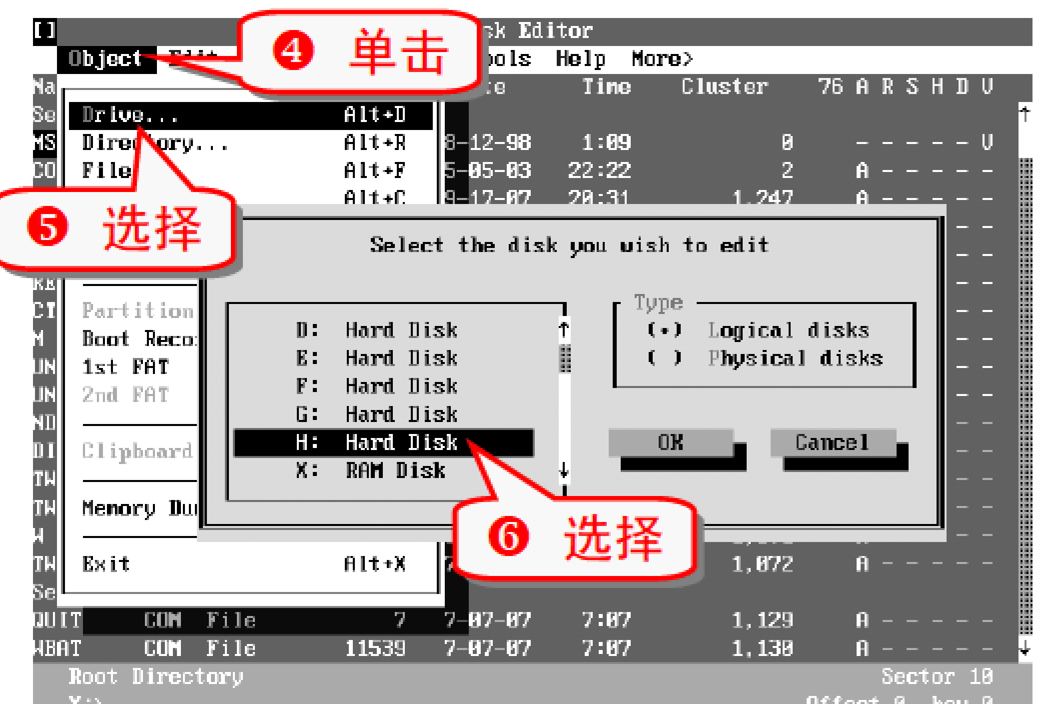
(1) 扫描子目录所在分区

❶ 将光盘放入光驱，重新启动电脑，在 BIOS 中将“第一启动顺序”设置为 CD-ROM，保存后退出 BIOS。

❷ 再次重新启动电脑，进入启动菜单选项。

❸ 选择“6. NU 2002 诺顿系列”，按下 Enter 键；选择“1. hinese”，按下 Enter 键；选择“1. DISKEDIT”，按下 Enter 键。





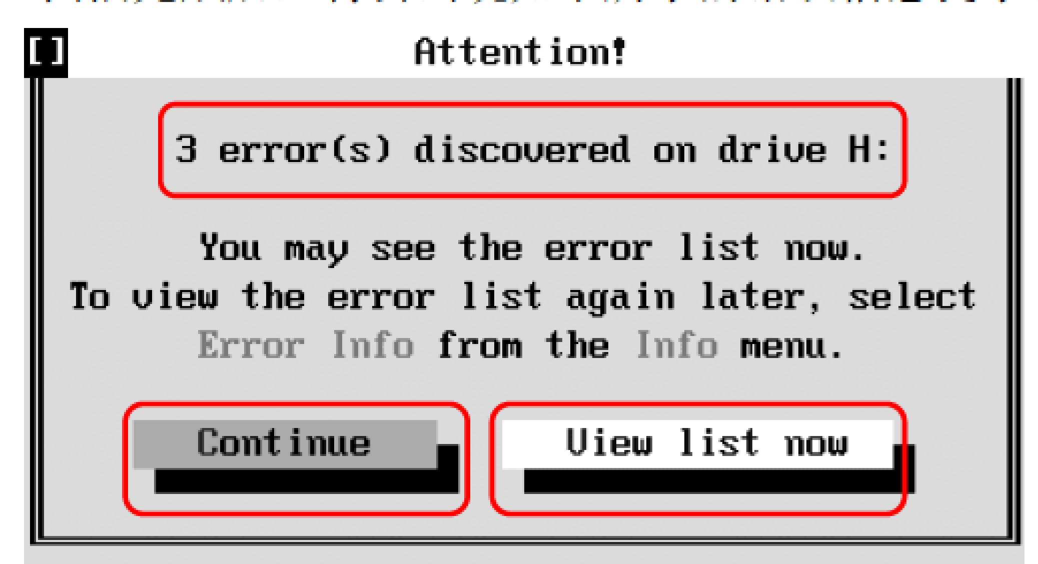
注 意 事 项

按下 Alt + O 组合键可直接打开 Object 菜单，选择 Drive...命令后需要按下 Enter 键才能进入选择分区的对话框，此处选择的是需要修复的子目录所在的分区。

❼ 按下 Enter 键开始扫描 H 盘。

(2) 查看错误信息

扫描完成后，将会出现如下所示的错误信息提示。



❶ 选择 Continue，按下 Enter 键显示 H 盘的文件和目录。

❷ 选择 View list now，按下 Enter 显示错误信息。



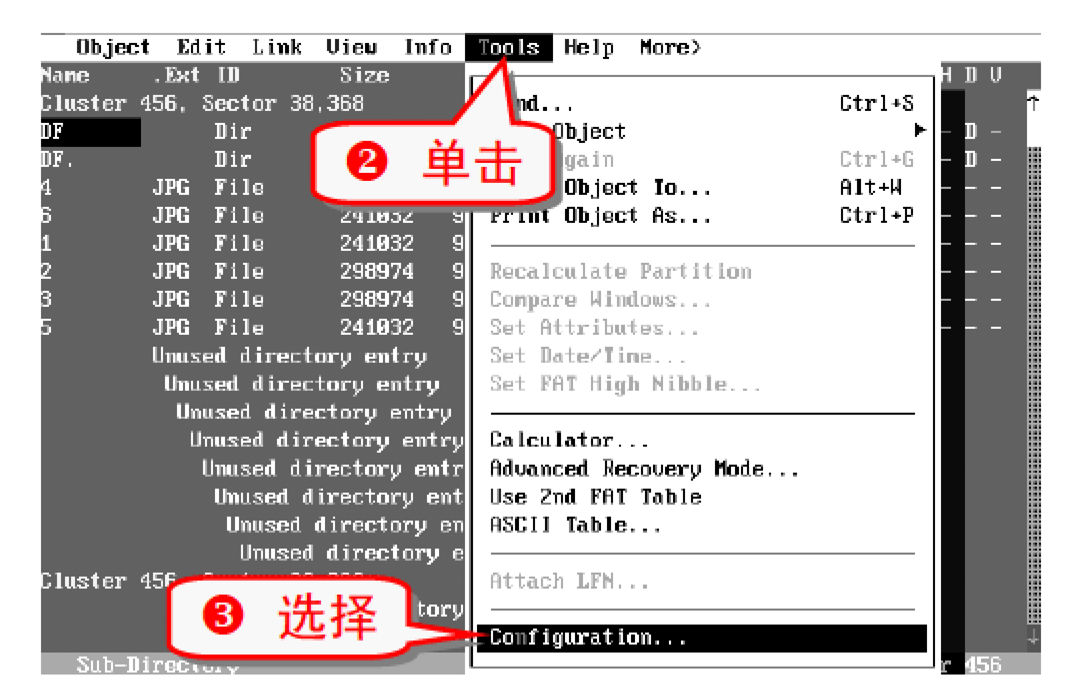
❺ 按下 Enter 键返回主界面。

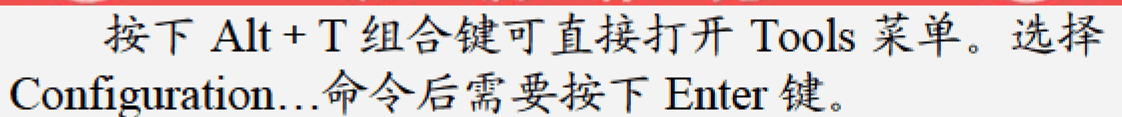
专 家 坐 堂

在 DOS 下使用键盘上的四个方向键可进行项目的选择，按下 Tab 键可进行前后项目的选择。按下 Alt + G 组合键，Disk Editor 可自动跳转到出问题的子目录。

(3) 修改损坏子目录

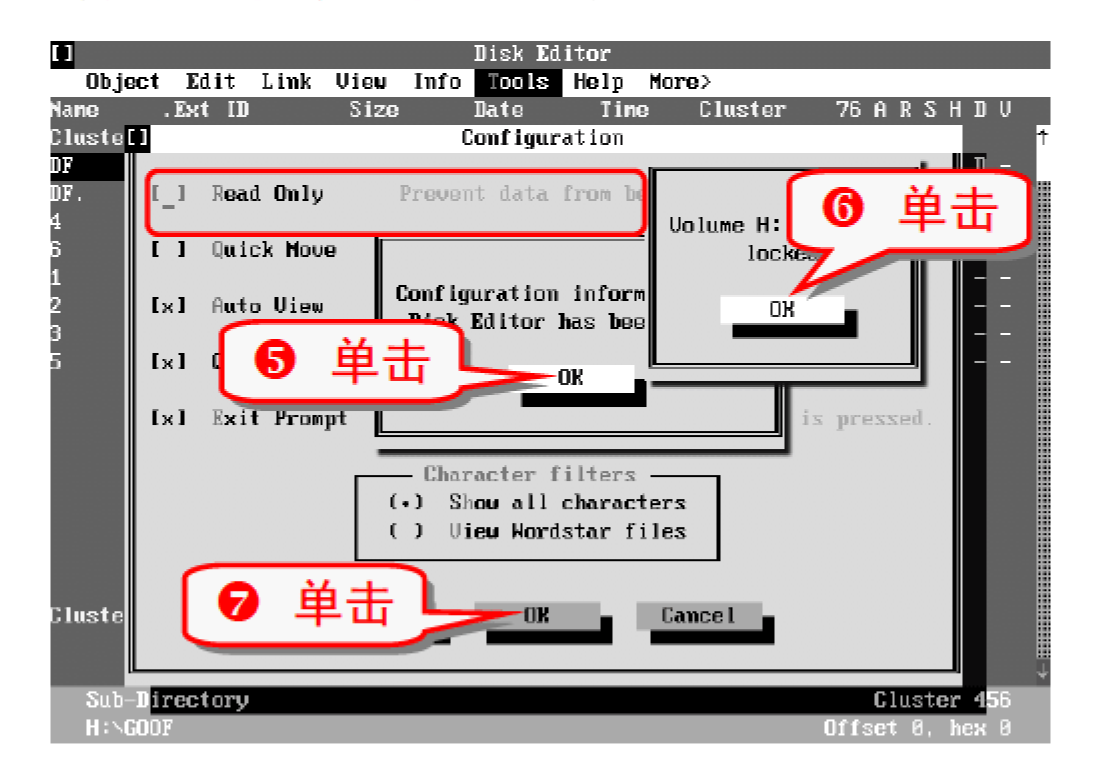
❶ 按下 Enter 键进入损坏的子目录。





按下 Alt + T 组合键可直接打开 Tools 菜单。选择 Configuration...命令后需要按下 Enter 键。

❹ 将光标移动到“[ ] Read Only”选项上，按下键盘上的空格键取消该选项，按下 Enter 键。



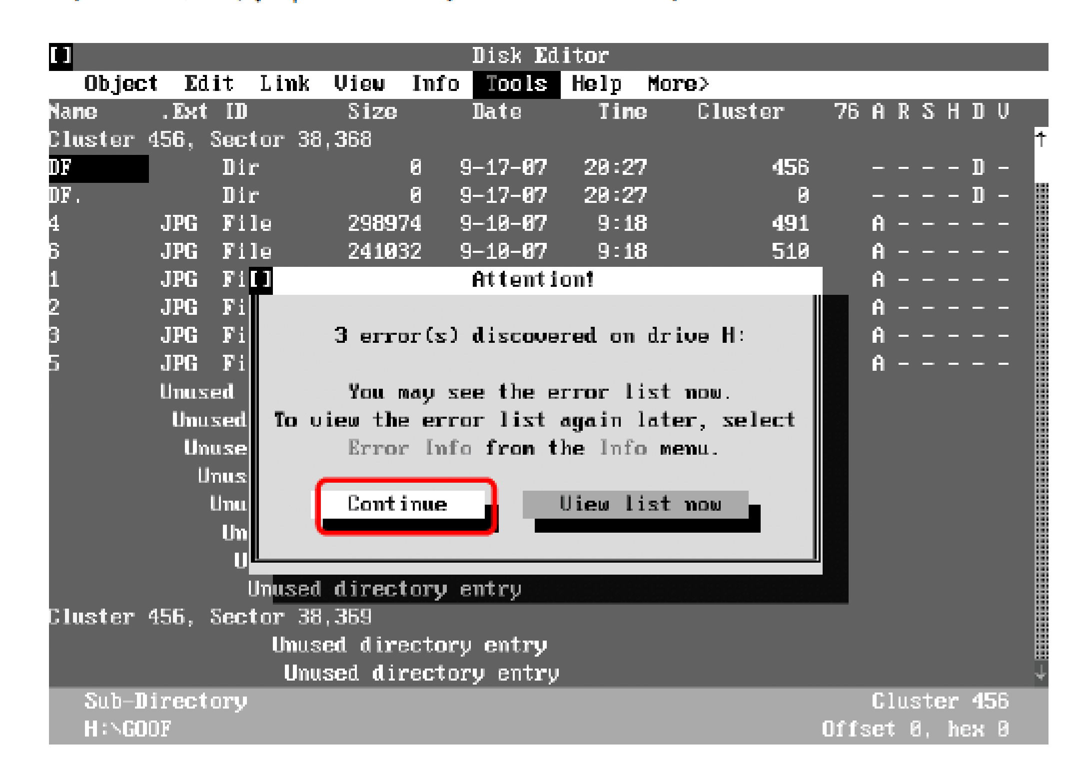




注　意　事　项

每次选择 OK 后需按下 Enter 键才能进入下一步操作。

❽ 选择 Continue 并按下 Enter 键，将第一项的 Name 改为“.”，将第二项的 Name 改为“..”。



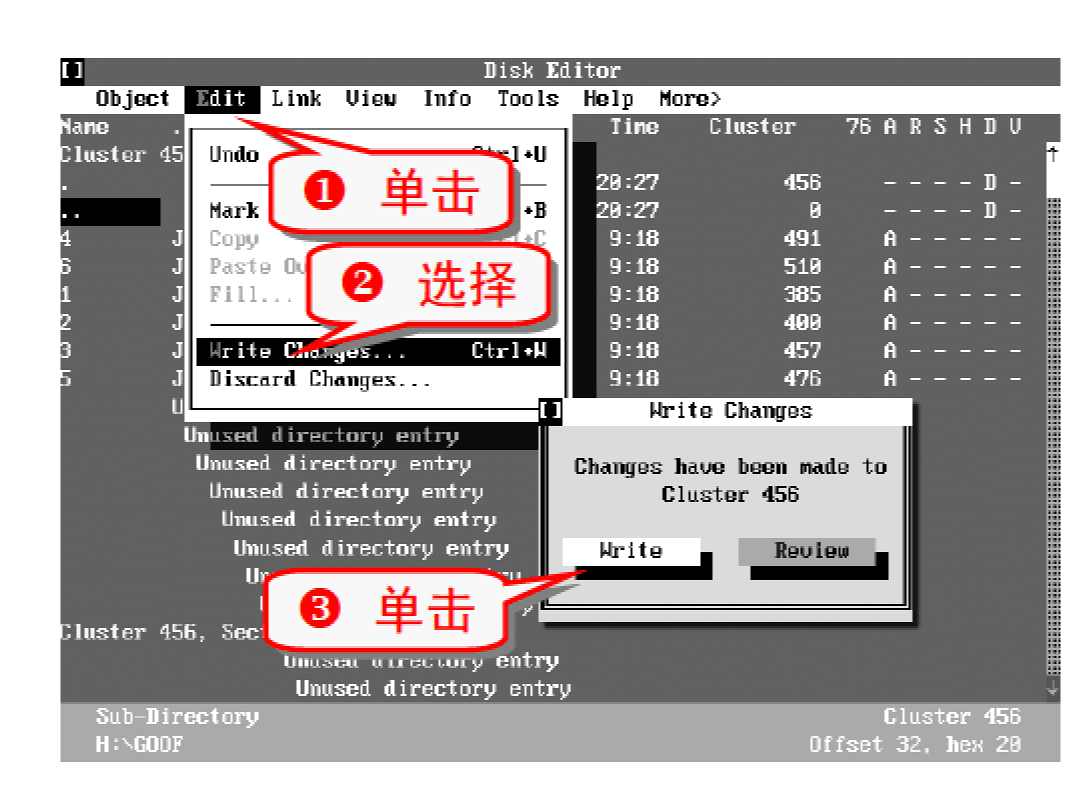



知　识　补　充

在 DOS 中使用 DIR 命令查询目录时，前两行的目录名分别为“.”和“..”。

(4) 保存修改并退出

修改完成后就可以进行保存并退出了。



❹ 按下 Enter 键。

❺ 按下 Alt + E 组合键退出 Disk Editor。

举　一　反　三

按下 Alt + E 组合键还可打开 Edit 菜单。

❻ 修改完成后重新执行 CHKDSK 命令检测磁盘，查看是否仍有“Invalid sub-directory entry(无效子目录项)”报告。



附录一　黑客常用命令

命　令	命令解析
arp -a	查看高速缓存中的所有项目
arp -a ***.***.*.*** 物理地址	向 arp 项目高速缓存中输入一个静态项目
arp –d ***.***.*.***	删除一个静态项目
attrib 文件名 +A +R +S +H	添加某文件的存档，只读，系统，隐藏属性
attrib 文件名 -A -R -S -H	去掉某文件的存档，只读，系统，隐藏属性
attrib 文件名(目录名)	查看某文件(目录)的属性
dir	查看文件
dir/Q	显示文件及目录属系统哪个用户
dir/T:A	显示文件上次被访问时间
dir/T:C	显示文件创建时间
dir/T:W	显示上次被修改时间
find 文件名	查找某文件
ipconfig	查看本地 IP 地址
ipconfig /all	显示全部配置信息
nbtstat -a ***.***.*.***	列出指定 IP 地址的远程机器名称表
nbtstat -a 计算机名	列出指定计算机名的远程机器名称表
nbtstat -n	列出本地 NetBIOS 名称
nbtstat -s	列出具有目标 IP 地址的会话表
net config	显示系统网络设置
net localgroup abc 123/add	把用户 abc 加入到 Administrator 组
net pause 服务名	暂停某服务
net send ***.***.*.*** “文本信息”	向 IP 地址为***.***.*.***的电脑发送信息
net share	查看当前电脑开启的共享
net share c$ /del	删除 C 盘共享
net share ipc$	开启 ipc$共享
net share ipc$ /del	删除 ipc$共享
net start	查看开启了哪些服务
net start 服务名	开启服务
net stop 服务名	停止某服务

续表

命 令	命令解析
net time ***.***.*.***	查看 IP 地址为***.***.*.***的电脑上的时间
net use ***.***.*.*** \IPC$	与 IP 地址为***.***.*.***的电脑建立 IPC 空链接
net use ***.***.*.*** \IPC$/del	删除与 IP 地址为***.***.*.***的电脑建立 IPC 空链接
net user	查看电脑中有哪些用户
net user abc 123 /add	添加一个用户名为 abc，密码为 123 的用户
net user guest /active:yes	将 guest 用户激活
net user guest 123	把 guest 的密码改为 123
net user guest/times:all	没有登录时间限制
net user 用户名	查看用户的属性
net user 用户名 /delete	删掉用户
net view	查看本地局域网内开启了哪些共享
net view ***.***.*.***	查看 IP 地址为***.***.*.***的电脑开放了哪些共享
netstat -a	查看开启了哪些端口
netstat -n	查看端口的网络连接情况
netstat -s	查看正在使用的所有协议使用情况
pause	暂停批处理程序
ping ***.***.*.*** (或域名)	向对方主机发送默认大小为 32 字节的数据
ping -t ***.***.*.*** (或域名)	一直 ping 指定 IP 地址或域名的电脑，按下 Ctrl+C 组合键结束 ping
route add	添加新路由项目到路由表
route change	修改数据的传输路由
route delete	从路由表中删除路由
route print	显示路由表中的当前项目
set	显示当前所有的环境变量
set a(或其它字符)	显示出当前以字符 a(或其他字符)开头的所有环境变量
set 指定环境变量名称=要指派给变量的字符	设置环境变量
taskmgr	调出任务管理器
tracert ***.***.*.*** -d	返回到达指定 IP 地址所经过的路由器列表



附录二　常见木马端口列表

端　口	木　马	端　口	木　马
31	Masters Paradise 木马	12223	Keylogger 木马
41	DeepThroat 木马	12345	NetBus 木马
58	DMSetup 木马	12346	GabanBus 木马
121	JammerKillah 木马	12361	Whack-a-mole 木马
138	隐形大盗	12362	Whack-a-mole 木马
146	FC-Infector 木马	12363	Whack-a-Mole 木马
456	Hackers Paradise 木马	12631	WhackJob 木马
531	RASmin 木马	13000	Senna Spy 木马
555	Ini-Killer 木马	13223	PowWow 聊天
560	远程监控	14500	PC Invader 木马
666	Attack FTP 木马	14501	PC Invader 木马
911	Dark Shadow 木马	14502	PC Invader 木马
999	DeepThroat 木马	14503	PC Invader 木马
1001	Silencer 木马	15000	NetDemon 木马
1010	Doly 木马	15382	SubZero 木马
1011	Doly 木马	16484	Mosucker 木马
1012	Doly 木马	16772	ICQ Revenge 木马
1015	Doly 木马	16969	Priority 木马
1024	NetSpy 木马	17072	Conducent 广告
1042	Bla 木马	17166	Mosaic 木马
1045	RASmin 木马	17300	Kuang2 the virus Trojan
1090	Extreme 木马	17449	Kid Terror Trojan
1095	Rat 木马	17499	CrazzyNet Trojan
1097	Rat 木马	17500	CrazzyNet Trojan
1098	Rat 木马	17569	Infector Trojan
1099	Rat 木马	17593	Audiodoor Trojan
1234	Ultors/恶鹰木马	17777	Nephron Trojan
1243	Backdoor/SubSeven 木马	19191	蓝色火焰
1245	VooDoo Doll 木马	19864	ICQ Revenge 木马
1349	BO DLL 木马	20001	Millennium 木马
1524	IngresLock 后门	20002	Acidkor Trojan
1600	Shivka-Burka 木马	20005	Mosucker 木马

续表

端　口	木　马	端　口	木　马
1807	SpySender 木马	20023	VP Killer Trojan
1863	MSN 聊天	20034	NetBus 2 Pro 木马
1981	ShockRave 木马	20808	QQ 女友
1999	Backdoor 木马	21544	GirlFriend 木马
2000	TransScout-Remote-Explorer 木马	22222	Proziack 木马
2001	TransScout 木马	23005	NetTrash 木马
2002	TransScout/恶鹰木马	23006	NetTrash 木马
2003	TransScout 木马	23023	Logged 木马
2004	TransScout 木马	23032	Amanda 木马
2005	TransScout 木马	23432	Asylum 木马
2023	Ripper 木马	23444	网络公牛
2115	Bugs 木马	23456	Evil FTP 木马
2140	Deep Throat 木马	23456	EvilFTP-UglyFTP 木马
2535	恶鹰	23476	Donald-Dick 木马
2565	Striker 木马	23477	Donald-Dick 木马
2583	WinCrash 木马	25685	Moonpie 木马
2773	Backdoor/SubSeven 木马	25686	Moonpie 木马
2774	SubSeven 木马	25836	Trojan-Proxy
2801	Phineas Phucker 木马	25982	Moonpie 木马
3024	WinCrash 木马	26274	Delta Source 木马
3050	InterBase	27184	Alvgus 2000 Trojan
3129	Masters Paradise 木马	29104	NetTrojan 木马
3150	DeepThroat 木马	29891	The Unexplained 木马
3700	Portal of Doom 木马	30001	ErrOr32 木马
4092	WinCrash 木马	30003	Lamers Death 木马
4267	SubSeven 木马	30029	AOL 木马
4567	File Nail 木马	30100	NetSphere 木马
4590	ICQ 木马	30101	NetSphere 木马
4899	Radmin 木马	30102	NetSphere 木马
5000	UPnP(通用即插即用)	30103	NetSphere 木马
5001	Back Door Setup 木马	30103	NetSphere 木马
5168	高波蠕虫	30133	NetSphere 木马
5321	Firehotcker 木马	30303	Sockets de Troie
5333	NetMonitor 木马	30947	Intruse 木马
5400	Blade Runner 木马	31336	Butt Funnel 木马
5401	Blade Runner 木马	31337	Back-Orifice 木马
5402	Blade Runner 木马	31338	NetSpy DK 木马
5550	JAPAN xtcp 木马	31339	NetSpy DK 木马
5554	假警察蠕虫	31666	BOWhack 木马
5555	ServeMe 木马	31785	Hack Attack 木马
5556	BO Facil 木马	31787	Hack Attack 木马
5557	BO Facil 木马	31788	Hack-A-Tack 木马
5569	Robo-Hack 木马	31789	Hack Attack 木马
5631	pcAnywhere	31791	Hack Attack 木马



续表

端　口	木　马	端　口	木　马
5632	pcAnywhere	31792	Hack-A-Tack 木马
5742	WinCrash 木马	32100	Peanut Brittle 木马
6267	广外女生	32418	Acid Battery 木马
6400	The Thing 木马	33333	Prosiak 木马
6667	小邮差	33577	Son of PsychWard 木马
6670	DeepThroat 木马	33777	Son of PsychWard 木马
6711	SubSeven 木马	33911	Spirit 2000/2001 木马
6771	DeepThroat 木马	34324	Big Gluck 木马
6776	BackDoor-G 木马	34555	Trinoo 木马
6939	Indoctrination 木马	35555	Trinoo 木马
6969	GateCrasher/Priority 木马	36549	Trojan-Proxy
6970	GateCrasher 木马	37237	Mantis Trojan
7000	Remote Grab 木马	40412	The Spy 木马
7070	RealAudio 控制口	40421	Agent 40421 木马
7215	Backdoor/SubSeven 木马	40422	Master-Paradise 木马
7300	网络精灵木马	40423	Master-Paradise 木马
7301	网络精灵木马	40425	Master-Paradise 木马
7306	网络精灵木马	40426	Master-Paradise 木马
7307	网络精灵木马	41337	Storm 木马
7308	网络精灵木马	41666	Remote Boot tool 木马
7511	聪明基因	46147	Backdoor.sdBot
7597	QaZ 木马	47262	Delta Source 木马
7626	冰河木马	49301	Online KeyLogger 木马
7789	Back Door Setup/ICKiller 木马	50130	Enterprise 木马
8011	无赖小子	50505	Sockets de Troie 木马
8102	网络神偷	50766	Fore 木马
8181	灾飞	51996	Cafeini 木马
9408	山泉木马	53001	Remote Windows Shutdown 木马
9872	Portal of Doom 木马	54283	Backdoor/SubSeven 木马
9873	Portal of Doom 木马	54320	Back-Orifice 木马
9874	Portal of Doom 木马	54321	Back-Orifice 木马
9875	Portal of Doom 木马	55165	File Manager 木马
9898	假警察蠕虫	57341	NetRaider 木马
9989	iNi-Killer 木马	58339	Butt Funnel 木马
10066	Ambush Trojan	60000	DeepThroat 木马
10067	Portal of Doom 木马	60411	Connection 木马
10167	Portal of Doom 木马	61348	Bunker-hill 木马
10168	恶邮差	61466	Telecommando 木马
10520	Acid Shivers 木马	61603	Bunker-hill 木马
10607	COMA 木马	63485	Bunker-hill 木马
11000	Senna Spy 木马	65000	Devil 木马
11223	Progenic 木马	65390	Eclypse 木马
11927	Win32.Randin	65432	The Traitor 木马
12076	GJammer 木马	65535	Rc1 木马